Registry Plus
Central Registry Tools

Web Plus, eMaRC Plus,
Prep Plus, and CRS Plus

Systems and IT Personnel Requirements

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

National Center for Chronic Disease Prevention and Health Promotion
Division of Cancer Prevention and Control

Contents

System Requirements for CRS Plus

CRS Plus is a client-server application which connects to the registry database on Microsoft SQL Server running on a server computer, and the client application that runs on individual workstations.

Database Server

The table below lists specifications for the database server computer, which is assumed to be installed within an existing, larger IT infrastructure with connectivity, security, and operational features established by local policy.

Note: This specification is for a dedicated server only. If other services and applications are running on this server, additional RAM and hard disk space may be required.

System Component	Database Server Computer
RAM	8 GB; more memory will result in better performance
Hard disk	RAID-5 for data, RAID-1 for log files
Size of data file	(3 * 7000 * estimated_number_of_cases) / 1048576 MB
Size of transaction log file	25% of the data file size
System drive for caching	At least 10GB of free space
CPU	Dual or greater processor
OS	Windows Sever 2012 (Server 2012 Enterprise will meet the NIST FIPS 140-2 standard) or later
Database server	SQL 2012 (Standard Edition) or later

Client PC

The table below lists specifications for the client computer.

System Component	Client Computer
RAM	2 GB or more
Hard disk	At least 1 GB of free space
OS	Windows 7/8/10
Applications	Microsoft Access 2000 or above, make sure scripts are permitted to execute

System Requirements for Prep Plus

Prep Plus is a .NET client-server application that connects SQL Server databases at the back end. The databases can be hosted on the same SQL server that hosts the CRS Plus database.

Database Server

The server used for CRS Plus database can also be used for Prep Plus. Some local temporary Microsoft Access databases can be located either on the client PCs or on a shared network drive. Some space is also required for storing text data files on the shared drive. The space required on the shared drive depends on the amount of data the central registry receives each year and how often the drives are archived.

Client PC

The table below lists specifications for the client computer.

System Component	Client Computer
RAM	2 GB or more
Hard disk	1 GB of free space
OS	Windows 7/8/10
Applications	Microsoft Access 2000 or above

Installing CRS Plus and Prep Plus

CRS Plus

You should have received a link to the FTP site and file information in an email from CDC. Download the installation file from the FTP site, double-click on it to start the installation wizard, and follow the screen prompts to complete the installation process. After installation, CRS Plus is accessible through the Start / All Programs / Registry Plus / CRS Plus menu.

To configure CRS Plus to work with a SQL Server database:

1. Prepare your database on Microsoft SQL Server:

    a. Create a database and database user account(s) on Microsoft SQL Server; the user account(s) should have both read and write access to all tables, and execute permissions on all stored procedures in the database.

    b. Run the script provided by CDC to create database objects.

2. Modify the connections.xml file:

a. Open Connections.xml file in the application folder.

b. Configure the connection string: Update database connection strings to point to the CRS Plus database on SQL server and to the locations of mdbs.

Prep Plus

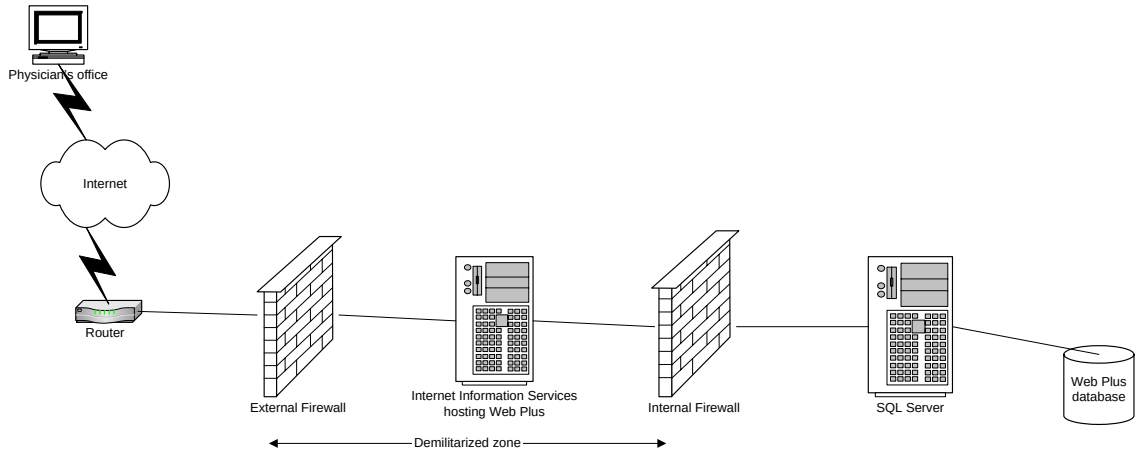
After downloading the installation file, double-click on it to start the installation wizard, and follow the prompts to complete the installation. After installation, Prep Plus is accessible through the Start / All Programs / Registry Plus / Prep Plus menu.

To use Prep Plus in a networked environment, modify PrepPlus.exe.config in the application folder to point several folder paths and databases to shared network drives.

If you have questions about setting up CRS Plus or Prep Plus, contact us at cancerinformatics@cdc.gov

System Requirements for Web Plus

Web Plus is a web application that runs on Microsoft Internet Information Services (IIS) and stores the data in a Microsoft SQL Server database. The application must be accessible from the public Internet with support for encrypted communication between clients and the web server. In a typical setup, one server computer hosts the application, and another runs SQL Server. Typically, the web server is placed in the demilitarized zone between the external and internal firewalls, and the SQL Server sits behind the internal firewall as part of the internal trusted network.



A router connects the demilitarized zone to the Internet. A Secure Sockets Layer (SSL) digital certificate is installed on the web server for site authentication and encryption of data transferred between the clients and the web server. The digital certificate can be created internally if a certificate server is available, or it can be purchased from a vendor. If the organization does not have a registered Internet domain, it needs to register one.

The table below lists specifications for web server and database server computers, which are assumed to be installed within an existing, larger IT infrastructure with connectivity, security, and operational features established by local policy.

Note: Fault-tolerant disks are recommended for the database. The RAM and hard disk free space requirements may increase if this server also hosts databases for other applications.

System Component	Web Server	Database Server
Processor	**Minimum:** 1 GHz (x86 processor) or 1.4 GHz (x64 processor) **Recommended:** 2 GHz or faster 64-bit processor	**Minimum:** 1 GHz (x86 processor) or 1.4 GHz (x64 processor) **Recommended:** 2 GHz or faster 64-bit processor
RAM	**Minimum:** 512 MB RAM **Maximum (64-bit systems):** 32 GB (Standard) or 1 TB (Enterprise and Datacenter) or 2 TB (Itanium-Based Systems) **Maximum (32-bit systems):** 4 GB (Standard) or 64 GB (Enterprise and Datacenter) **Recommended:** 2 GB RAM or more	**Minimum:** 512 MB RAM **Maximum (64-bit systems):** 32 GB (Standard) or 1 TB (Enterprise and Datacenter) or 2 TB (Itanium-Based Systems) **Maximum (32-bit systems):** 4 GB (Standard) or 64 GB (Enterprise and Datacenter) **Recommended:** 2 GB RAM or more
Hard disk	**Minimum:** 10 GB Recommended: 40 GB or more	**Minimum:** 10 GB **Recommended:** 40 GB or more
Operating system	Microsoft Windows 2008 Server or later	Microsoft Windows 2008 Server or later
Microsoft IIS	7.0 or later	Not applicable
.NET Framework	Version 4.5 or later	Not applicable
SQL Server	Not applicable	Microsoft SQL Server 2008 (standard edition) **Recommended:** SQL Server 2012 or SQL Server 2016
SSL Certificate	Install the SSL digital certificate on this server. SSL/TLS is the underlying technology that secures transmitted data on the Internet. Some configurations of SSL/TLS have known weaknesses that could allow an attacker to compromise their security and IIS enable weak protocols and ciphers by default. As a result, web server administrators must make changes to ensure a secure implementation of SSL/TLS. The SSL 2.0 and SSL 3.0, TLS 1.0, TLS 1.1 must be disabled and make sure TLS 1.2 protocol is enabled.	Not applicable

Web Plus Security Features and Recommendations

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 of Web Plus.

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 configurations of 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 (and their assigned roles) who have access to the Web Plus application and the database. 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 sharing accounts should be expressly prohibited.

Security Features of the Web Plus Application

Authentication

Web Plus uses form-based authentication, which requires users to enter their user ID and password. Multi-factor authentication can be implemented by requiring users to enter a personal identification number and/or answer challenge questions in addition to providing their user ID and password.

Passwords

Web Plus provides several options to configure passwords, which can be set by central registry administrators. Attributes that can be configured are:

- Enforce the complexity of passwords using a regular expression.
- Keep a history of passwords and require that new passwords be different from old ones.
- Force users to change their passwords after a specified time interval.
- If an administrator resets a user's password, Web Plus may force the user to change the password immediately upon login.

Personal Identification Number (PIN)

When enabled on the systems preference page, this option allows central registry administrators to generate a unique PIN matrix for every Web Plus user. To log in, in addition to

their user ID and password, users must enter a four-digit PIN based on coordinates from their PIN matrix, which is mailed to users by the hosting agency.

Challenge Questions

When enabled on the systems preference page, central registry administrators can enter challenge questions that each user must answer when the feature is initially enabled, and then entered upon login to validate the user's identity. The number of challenge questions can be specified.

Role-Based Access

Web Plus also implements role-based access that grants users different levels of access depending on the role or roles assigned to them. Seven roles are defined in Web Plus:

- **Facility abstractor:** Works in a local facility or doctor's office and handles patients' medical records and paperwork. When a patient is diagnosed with cancer, the facility abstractor reports the case to the state's central cancer registry.

- **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 local facilities with access to Web Plus to report their data; manages facility accounts and users at both the 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:** Manages local users of a facility.

- **File uploader:** Uploads files of abstracts in the appropriate NAACCR format that were not abstracted using Web Plus, views the EDITS error report and cleans, or works with abstractors to clean, errors on rejected files prior to re-uploading.

- **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.

Other Application Security Features

Other security features of the application include:

- Facilities and offices have access only to 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 configurable value.
- A user account can be deactivated temporarily.
- User activities are visible to central registry administrators through the Current User Activities page.
- Display types and edit set configurations are controlled centrally.
- User passwords are stored in the database using a one-way hash algorithm.
- The Web Plus configuration file can encrypt the connection string to the SQL Server database.

Security of the Operating Infrastructure

Security on the Client Computer

The client computer should be protected from 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 to protect data exchanged over the Internet. To set up an SSL channel, a server certificate must be installed on the web server, and the website containing the application should have SSL encryption turned on. The certificate for the server can 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 with Client Certificates

In addition to their user ID and password, 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.

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 encrypted using DPAPI in web.config. If Windows authentication is used, the user's credentials are not included in the connection string, but the connection string is still encrypted to hide the database server's IP address, port number, and other information.

Windows authentication is the preferred method because the user's credentials are not transmitted over the network. In order 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 installing .NET Framework on the web server. By default, all ASP.NET applications run under the security context of this account. 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 should be opened in the internal firewall to allow the 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.

Installing Web Plus

IMPORTANT: Web Plus has not been tested in the load-balanced environment. Please contact CDC if you want to test it in this environment. A Windows 2008 or newer server operating system is highly recommended for production use of Web Plus because of improved security and stability of these operating systems.

1. Initial steps:

    a. Set up a web server computer on your network with the Internet Information Services (IIS) and .NET Framework version 2.0 installed. If you have Windows 2008 or later server versions, change your server configuration to add the web server (IIS) role and enable it to run ASP.NET applications.

    b. The web server should have proper connectivity to a SQL Server computer. SQL Server and the web server can be located on the same computer for testing purposes.

    c. Create a user account (SQL Server account or Windows domain account) on the SQL Server for all Web Plus users to access the Web Plus database from the application.

    d. If your web server sits outside the firewall and the SQL Server is inside the firewall, open appropriate ports on the firewall to let the web server and the SQL Server communicate with each other.

2. Download the Web Plus deployment files (filename will appear in the email you received) from the specified folder on CDC's FTP site:

    Address: ftp://sftp.cdc.gov
    UserID: nccdnc
    Password: 2013cDast

3. Unzip the downloaded file to a temporary folder.

4. Create and configure the database for Web Plus on the database server computer.

    a. A SQL Server backup is included in the deployment package in the WebPlusV2\Data folder. Create the WebPlus database from this backup.

    b. Grant the "datareader" and "datawriter" roles to the Web Plus user account; also grant this account the execute permission on stored procedures called "lookupuser", "initializelargeobjectstableforinsert", and "getsetbaseid".

    NOTE: The above instructions are for Microsoft SQL Server 2008 and later versions. A version of Web Plus is available that works with My SQL Server, but all functions of the application have not been tested to work correctly with this database. If you are using a My SQL Server database, download the My SQL Server version of the application. The

deployment package has a MySQL data dump in the WebPlus\data folder. Create a WebPlus database from this dump and update the database connection string in the web.config file (WebPlus folder) to point to this database.

5. Set up the application on the web server. The steps for this task differ depending on the operating system on the web server. Please locate the section for the operating system you have on the web server and follow the steps described in that section.

   Windows 2008 Server Editions:

   a. Create a folder on the web server and copy all of the unzipped files and sub-folders from the temporary folder created in step 3 to this folder on the server.

   b. Open the web.config file in the above folder and modify the “dbconnection” key value under “appsettings” to point to your SQL Server database and the “smtpserver” value to your SMTP server IP address.

   c. Using Internet Information Server (IIS) Manager, add an application folder under Default Website. In the dialog box, specify an alias (such as WebPlus), select the preconfigured Classic Application Pool or another application pool you may have created for Web Plus, and the physical path of the Web Plus folder created in step 5.a above. If multiple web applications are running on this web server, consider creating a separate application pool for Web Plus.

   d. Select the application pool to which Web Plus belongs and set it to run .NET Framework v2.0 in the Classic Pipeline mode. If you chose the preconfigured Classic Application Pool in step 5.b, both of these options are already set. This setting is available from the Basic Settings menu of the application pool.

   e. Select the application pool to which Web Plus belongs and set the recycling conditions to recycle at a specific time, preferably sometime after midnight when few are likely to be using the application, and uncheck all other recycling conditions. The recycling conditions option is available from the Recycling menu of the application pool.

   f. Set the idle time-out option to disable worker process time-out. This option is available under the Process Model group in the Advanced Settings menu of the application pool.

   g. If using Windows 2008 64-bit server, set the application pool to run the 32-bit application. This option is available from the Advanced Settings menu of the application pool.

   Windows 2003 Server Editions:

   a. Create a folder on the web server and copy all of the unzipped files and sub-folders from the temporary folder created in step 3 to this folder on the server.

b. Open the web.config file in the above folder and modify the “dbconnection” key value under “appsettings” to point to your SQL Server database and the “smtpserver” value to your SMTP server IP address.

c. Create a new virtual directory under Default Web Site, specify an alias name (such as WebPlus), point to the physical path of the Web Plus folder created in step a. above, and allow read and run script permissions on the virtual folder.

d. Open the Properties dialog box of the virtual directory created in step b. and set its Application Pool property to the application pool you may have created for Web Plus. If multiple web applications are running on this web server, consider creating a separate application pool for Web Plus. The DefaultAppPool is selected by default. Select ASP.NET tab on the Properties dialog box and select 2.x for ASP.NET version. If you do not see the ASP.NET tab on this dialog box, you may not have installed .NET Framework v2.x on the server. When .NET Framework 2.x is installed, the ASP.NET tab is added to the Properties dialog box.

e. Select the application pool to which Web Plus belongs (DefaultAppPool by default), open the Properties dialog box, and set the properties as follows:

   - Under the Recycling tab, uncheck the “Recycle worker processes (in minutes)” and “Recycle worker processes (number of requests)” checkboxes. Check the “Recycle worker processes at the following times” checkbox and specify the time when worker processes can be recycled safely, preferably sometime after midnight. Uncheck both checkboxes under the Memory Recycle group.

   - Under the Performance tab, uncheck the idle timeout option.

   - Leave other application options at their default values.

6. Start ASP.NET State Service:
   Web Plus stores session variables in the State Server. Start ASP.NET State Service by going into Services and set it to start automatically.

7. Test Web Plus:

   a. Enter http://webserveraddress/virtual_folder/logonen.aspx in the address bar of a browser. The first time you access the site, it will take a few seconds as Web Plus initializes and brings up the login page.

   b. Enter “johndoe” as the user ID and “abstractor” as the password.

8. Install the Web Plus Administration Tool on the central registry administrator’s PC.

The Web Plus Administration Tool

Abstracts that are entered, completed, and released via Web Plus are stored in the SQL database, which resides inside the internal firewall. Files of abstracts that are uploaded via Web Plus are also stored in the SQL database. Abstracts and uploaded files (bundle submissions) need to be exported out of the SQL database so they can be imported into the central cancer registry database.

Because Web Plus runs on a web server that sits outside the internal firewall, for enhanced security and performance there is a separate Windows application to export files of abstracts and uploaded files called the Web Plus Administration Tool. Because this application runs in the same LAN where the Web Plus database resides, files can be exported out of the database rapidly. In addition, the Web Plus Administration Tool provides an added layer of security---it can only connect to the database when it is running inside the firewall, so access to the export function is limited to local users.

The Web Plus Administration Tool can also be used to run scheduled, batch edits on uploaded files, as well as to run edits manually on any uploaded file in NAACCR file format.

Installing the Web Plus Administration Tool

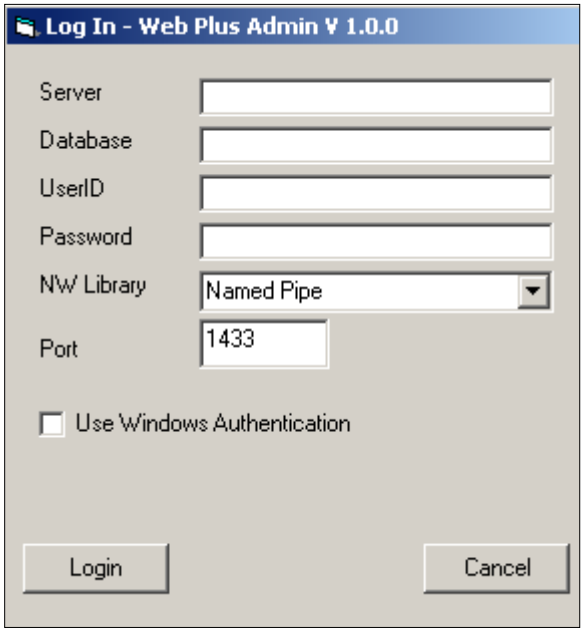
Note: .NET Framework version 2.0 must be installed on the PC on which you would like to install the Web Plus Administration Tool.

To install the Web Plus Administration Tool on the central registry administrator's PC, follow these steps:

1. Download the Web Plus Administration Tool installation program from CDC's FTP site. You should have received the folder and the name of the latest installation file in an email.
2. Double-click on the installation program file to begin the installation process, and follow the prompts to complete the installation. The installation program will create a menu entry called "Web Plus Administration" under the Start / All Programs menu.
3. Locate WebPlus.ini file in the C:\Windows folder and update the database connection string to point to your Web Plus database.
4. To launch the Web Plus Administration Tool, click on Start / All Programs / Web Plus Administration / Web Plus Admin Tool.
5. Obtain the SQL Server name, database, user ID (SQL Server login), and password; the administrator will enter this information when the Web Plus Administration Tool is launched in order for it to connect to the SQL server. This information is only required the first time this application is run. For subsequent runs, only the central registry administrator's user ID and password are required to log in.

Initial Login to the Web Plus Administration Tool

To launch the Web Plus Administration Tool, click on Start / All Programs / Web Plus Administration / Batch Processing. Upon initial login, the Log In dialog box opens.

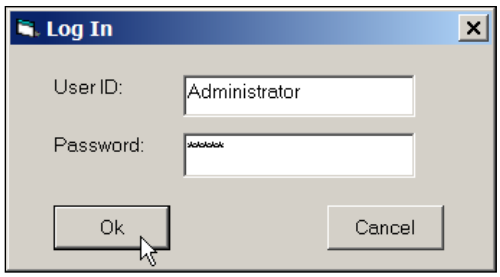


Enter the following information in each field:

- **Server:** Name or IP address of SQL Server.
- **Database:** Name of SQL database.
- **UserID:** SQL Server login ID.
- **Password:** Password for SQL Server.
- **NW Library:** Select a network library to use (Named Pipe or TCP/IP).
- **Port:** The port number SQL Server listens on (1433 is the default).
- **Use Windows Authentication:** Check this box if you are using Windows authentication. There is no need to enter the UserID and password if this box is checked.

Click the **Login** button to launch the Web Plus Administration Tool.

Upon future logins, only the central registry administrator's user ID and password are needed:



System Requirements for eMaRC Plus

eMaRC Plus is a file mapping tool that is used to view and work with pathology lab files in HL7 or pipe-delimited format. The application imports HL7 files manually or directly from the PHIN Messaging System (PHINMS) queue, and tests the messages for existence of required data items. eMaRC Plus searches for cancer terms to mark potential cancer cases, and builds a pathology lab database in SQL Server.

eMaRC Plus reads HL7 version 2.3.1 ORU^01 message batch files, parses messages, and stores HL7 data elements as discrete field values into tables in the eMaRC Plus database. In a typical setting, the PHINMS is used to send HL7 batch files from a laboratory to a cancer registry or another agency working on the cancer registry's behalf. eMaRC Plus sits at a workstation at a cancer registry and polls the worker queue of the PHINMS receiver for any new incoming files. When a new file arrives in the queue, the application processes it and waits for another new file. eMaRC Plus can also be used in an interactive mode where the user selects a file to import into the eMaRC Plus database.

During import, the program searches a terms table to find a potential report of cancer; an inbuilt negation terms finder algorithm (NegEx) enhances the program's text mining capabilities in terms of specificity. The program shows imported pathology reports in a user-readable format with cancer terms highlighted in red and negated terms highlighted in blue. Both the terms table and the negation phrases table are customizable.

eMaRC Plus also creates partial abstracts from HL7 messages during import, translating various coded values from the HL7 coding standard to NAACCR standards. eMaRC Plus provides the ability to view both pathology reports' data items from HL7 messages and abstracts data items side-by-side on the same screen, and allows the user to look at the text of pathology reports and code data items, like primary site and histology, in partial abstracts. The auto-code histology feature suggests pertinent histology codes by analyzing the text of the report while the user codes abstracts.

The table below lists specifications for the client PC on which eMaRC Plus is installed. If you use databases other than SQL Server LocalDB, you will need a server computer to host the database. This database can be put on the same server that hosts the CRS Plus, Prep Plus, and Web Plus databases.

eMaRC Plus Client PC

System Component	Client Computer
RAM	4 GB or more
Hard disk	At least 10 GB of free space
OS	Windows 7, Windows Server 2008R2 or later
.NET Framework	Version 4.5 or later

Database Server

The table below lists specifications for the database server computer, which is assumed to be installed within an existing, larger IT infrastructure with connectivity, security, and operational features established by local policy.

Note: This specification is for a dedicated server only. If other services and applications are running on this server, additional RAM and hard disk space may be required.

System Component	Database Server Computer
RAM	8 GB, more memory will result in better performance
Hard disk	RAID-5 for data, RAID-1 for log files
Size of data file	(3 * 7000 * estimated_number_of_cases) / 1048576 MB
Size of transaction log file	25% of the data file size
System drive for caching	At least 0GB of free space
CPU	Dual or quad processor
OS	Windows Sever 20012 or higher (Server 20012 Enterprise will meet the NIST FIPS 140-2 standard)
Database server	SQL 2012 or higher

Installing or Upgrading eMaRC Plus

If you have a previous version of eMaRC Plus (or Mapper Plus as it was previously named) installed, you will need to uninstall the previous version before installing the new version.

You should have received the FTP site and file information in an email from CDC. Download the installation file from the FTP site, and double-click on it to install the program.

eMaRC Plus requires Microsoft .NET Framework 2.0 or above to be installed on the computer. If you are using a database other than Microsoft SQL Server, you may also need to install client connectivity software. You can unselect the Database Engine since you do not require SQL Server Express as a service.

After eMaRC Plus, LocalDB, and .NET Framework are installed, you can start the program from the Start menu / All Programs / Registry Plus / eMaRC Plus / eMaRC Plus.

If you are upgrading from a previous version, you may need to run database scripts to update the pathology database. Please refer to the release notes with the installation file to determine which database scripts you need to run.

This installation package contains eMaRC_Plus.mdf and eMaRC_Plus.ldf, which allow the Microsoft SQL Server LocalDB database to store pathology data; the application is configured to use this database by default. To create initial database objects in other database management

systems, ask your SQL Server database administrator to attach eMaRC_Plus.mdf and eMaRC_Plus.ldf to SQL Server. Your administrator can provide connectivity information, which must be updated in the C:\eMaRCPlus\MyConfig.cfg file. You may also have received an email telling you where to get the latest database scripts to create initial databases in different database systems.

You must have SQL Server Management Studio if you want to access eMaRC Plus directly. SQL Server Management Studio is not needed for normal operation.

The eMaRC Plus Database

eMaRC Plus imports HL7 batch files, parses the messages, and stores HL7 data elements to tables in the eMaRC Plus database. A mapping table called DATAMAP contains the mapping of HL7 data elements to fields of tables (refer to the Local Customization section below to see how states can use this table to select additional data items for storage). There are seven data tables—MSH, PV1, PID, ORC, OBR, OBX, and OBXCOMBINEDTEXT—the first six of which correspond to the six segments of the ORU^01 message. Data elements can be stored at the field, component, or sub-component level. The hierarchical relationships among segments are maintained in the database.

To simplify processing and use of text data, in addition to the OBX table which stores data elements of individual OBX segments as separate records, the text field (OBX-5) of all OBX segments that belong to an OBR segment are combined and inserted as one row in the OBXCOMBINEDTEXT table. This table has eight fields to store texts of the OBX segments, and depending on the LOINC code in the OBX-3 field, the text of OBX-5 will go into one of these eight text fields.

Raw HL7 messages are also saved to the HL7MESSAGES table.

Supported Database Types

eMaRC Plus has been tested to run on Microsoft SQL Server 2008R2 to SQL Server 2016. When initially installed, by default eMaRC Plus is configured to use the SQL Server LocalDB database that is packaged with the installation file. The LocalDB can be up to 10 GB maximum. It is highly recommended that the eMaRC Plus database be put on a more robust centralized SQL Server database 2012 or newer. If you plan to continue using LocalDB for production work, we recommend using BitLocker to secure your entire client computer.

Configuring eMaRC Plus

eMaRC Plus comes preconfigured with some default settings so that the program can be run immediately after installation. Before using eMaRC Plus in production, you should configure it to suit your environment and preferences.

The configurations are set in the Configuration dialog box, which can be accessed from the System Configuration menu item under the Administration menu. The following options can be set:

Pathology Reports (ePath) Database Connection String: SQL Server Connection string to the Pathology Reports database. This is the main database that stores imported messages and parsed data values from messages. This database also contains the DATAMAP table, lookup tables, translation tables, and other parameter tables. The default value points to a SQL Server LocalDB, which is included with the installation. The typical way of connecting to the SQL Server database follows; please contact your database administrator for connection values.

Typical connection string:

SERVER=Server IP address or name; DATABASE=eMaRCPlus database name; UID=database user ID; PWD=database password; MultipleActiveResultSets=true;

If database access is controlled using Active Directory, please use:

SERVER=Server IP address or name; DATABASE=eMaRCPlus database name; Trusted_Connection=true; MultipleActiveResultSets=true;

Important: This installation package contains eMaRC_Plus.mdf, which is the starter Microsoft SQL Server LocalDB to store pathology data. By default, the application is configured to use this database. LocalDB can be moved easily to the SQL Server Enterprise version. If you upgrade from LocalDB to the Enterprise version, move eMaRC_Plus.mdf and eMaRC_Plus.ldf to the centralized SQL Server.

PHIN Worker Queue (PHINMS Queue) Connection String: This database is where the PHINMS worker queue is located. This database must be SQL Server 2008R or newer. By default, the application is pointing to LocalDB, called PHINMS.mdf, included in the installation folder. It is highly recommended that databases for pathology reports and PHIN Worker Queue are kept separate, but you can put both databases on the same SQL Server and use different connection strings.

Typical connection string:

SERVER=Server IP address or name; DATABASE=PHINMS database name; UID=database user ID; PWD=database password;

If database access is controlled using Active Directory, please use:

SERVER=Server IP address or name; DATABASE=PHINMS database name; Trusted_Connection=true;

Worker Queue Name: Enter the PHINMS Worker Queue name, for example, ELRWorker Queue. Please check with your PHNMS implementation team to find what the queue name is.

PHINMS File Receive Folder Path: If your PHINMS receiver has been configured to store received files in a folder, enter the folder path where the received files are stored. The

preferred setting in the PHINMS Receiver is not to store files in a folder, but rather to leave files in the database in the message queue table.

Read File from the PHINMS Queue: This is the default and preferred option. Selecting this option will make the program read the incoming file from the worker queue.

Service Code: Service code to identify the file in the PHINMS worker queue, for example, ELR_HL7231. Please check with your PHNMS implementation team to find what your service code is.

Archive Folder: eMaRC Plus copies the imported file to this folder before processing it.

Cancer Terms Search Options: Available under the Reports Filtering and Auto-coding tab.

- **Write all cases to the database without filtering:** Writes all messages to the database without searching for cancer terms in the OBX texts of the messages.
- **Write all cases to the database and flag non-reportable cases:** Writes all messages to the database, but flags non-reportable reports with a different status code.
- **Write only reportable cases to the database:** Excludes any messages that do not have cancer terms in their OBX texts.

Text Sections to Search for Filtering: Check the sections you want eMaRC Plus to search for cancer terms. By default, all sections are checked.

Text Sections to Search for Auto-Coding: Check the sections you want eMaRC Plus to examine to suggest histology codes. By default, all sections are checked.

eMaRC Plus Local Customizations

States can customize eMaRC Plus to change the data items that are stored as discrete fields in the database tables, and whether they are required or optional.

DATAMAP table: eMaRC Plus uses this table to find which HL7 data elements are stored in which fields of data tables. Many of the fields in this table are used only for documentation. The following fields are used for site-specific configuration:

DataTableName: The table name where each HL7 data element is stored. MSH, PV1, PID, ORC, OBR, and OBX are valid values.

DataFieldName: The field name where each HL7 data element is stored. The field name should exist in the table.

NAACCROpt_xxxx: Optionality column; defines whether data elements are required (R), required when available (R*), or optional (O). You can have a separate optionality column for

each laboratory from which your site receives messages. Use the **PREFERENCES** table to show which optionality column each laboratory uses.

For example, if you store PID.3.4 as a separate entity in the database, follow these steps:

1. Open the **DATAMAP** table and locate PID.3.4 under HL7Element.
2. Enter PID under DataTableName.
3. Enter AssigningAuthority (or any other name that is meaningful to you) under DataFieldName.
4. Update the optionality column for each laboratory if required to change the default value.
5. Update the length field to indicate the maximum length for this field.
6. Open the PID table in the design view and add a field called AssigningAuthority to this table with the datatype text (or varchar depending on the database you are using) and the field length specified in step 5 above.

PREFERENCES table: This table shows a mapping of laboratories and optionality columns in the DATAMAP table.

IT Personnel Requirements and Recommended Availability to Support Registry Plus Central Registry Tools

The central registry will need people with experience in one or more of the following areas to provide IT support for Web Plus, eMaRC Plus, Prep Plus, and CRS Plus:

- Server administration.
- General IT support.
- Database administration.
- Network security.
- Web administration.

In a typical setting, IT support personnel will perform the following routine installation and support tasks:

Server Administration

Setting Up and Maintaining Servers

Each registry **must** have access to server hardware and IT support personnel for the server. These tasks are best performed by an experienced server administrator; this person is extensively involved during the initial setup of the server, and initially involved in establishing application connectivity.

- Initial server setup (if necessary).
- Perform day-to-day management of the server operating system.
- Test and deploy server equipment software and updates.
- Profile and monitor assigned servers.
- Maintain server performance.
- Meet on-call expectations, including off-hour support.
- If applicable, help oversee the physical security, integrity, and safety of the server environment.

Ongoing: The number of hours depends on local infrastructure, policy, and server environment.

General IT Support

Each registry **must** have access to IT personnel who can perform these tasks. They should be readily accessible, as these tasks may need to be performed frequently. These tasks typically

require about one half-hour for each installation or upgrade. Initial setup of applications may take longer. One person should be able perform these tasks.

Installing and Upgrading Desktop Applications

Installs CRS Plus, Prep Plus, and eMaRC Plus on workstations. Must have administrative rights to users' computers and be able to download files from CDC's FTP site.

Running Database Scripts and Performing Minor Database Modifications

Some application upgrades may require database changes. If so, CDC will send the scripts and procedures required to make these changes, and the responsible IT personnel should be able to use SQL Management Studio to run the scripts and make database changes. Ideally, this person also can write simple SQL scripts to satisfy data requests from registry users.

Start-up/conversion: 32 hours of general IT support
Ongoing: Four hours per month of general IT support

Database Administration

Each registry **must** have access to IT personnel who can perform these tasks, preferably an experienced database administrator. This person is extensively involved during the initial setup of the applications, and afterward makes backups and maintains the database following the practices of the local data processing center.

Creating and Administering Databases on the SQL Server

For the initial setup, creates databases on a Microsoft SQL Server and subsequently performs regular maintenance and backups. This person should be able to write SQL scripts to get counts, create specialized extracts, and perform direct updates to the database in response to requests from registry users.

Start-up/conversion: Eight hours of database administrator support
Ongoing: Four hours per month of database administrator support

Network Security, Web Administration, and Database Administration

Setting Up and Upgrading Web Plus on the Web Server

Each registry implementing Web Plus **must** have access to IT personnel who can perform these tasks. When Web Plus is initially set up, the web administrator works with network security and database personnel to establish connectivity with the database and mail server. Initial setup typically takes four hours if the operating systems are already installed on the servers and are connected to the network. Subsequent upgrades to applications can be done in less than an hour.

The responsible IT personnel should be able to set up Web Plus in IIS and perform upgrades as newer versions become available, and should be able to perform any recommended .NET framework upgrades.

Start-up/conversion: Four hours of network/security support, four hours of web administrator support, and four hours of database administrator support

Ongoing: Two hours per month of web administrator support and two hours per month of database administrator support

Writing Special Programs (Optional)

If the functionalities within CRS Plus and Prep Plus are not sufficient to meet the needs of the registry, the registry may require a programmer to manipulate files and data and to create special reports.

Ongoing: Number of hours depends on tasks

Installing and Administering Applications on the Terminal Server (Optional)

CRS Plus, Prep Plus, and eMaRC Plus can be installed in the terminal server environment (Windows terminal server or Citrix application server), which eliminates the need to install these applications on individual workstations. Because of reduced need for IT support, installing applications in the terminal server environment is recommended if such an environment is available.

If the applications are installed on a terminal server, the IT personnel administering the server should be available for application upgrades and to maintain user accounts on the terminal server.

Start-up/conversion: Eight hours of terminal server administrator support
Ongoing: Four hours per month of terminal server administrator support