Greenway PrimeSUITE 17
System Requirements

Confidential

This document and the information it contains are the confidential information of Greenway Health. Neither this document nor the information it contains may be disclosed to any third party or reproduced, in whole or in part, without the express prior written consent of Greenway.

Greenway reserves the right to change, without notice, product offerings, product specifications and the information in this document. This document supersedes any prior document containing similar subject matter with regard to the descriptions of features and functionality of product offerings. You may receive supplements to this document based on changes that may occur in the product. This document may not be reproduced in any form without prior written permission from Greenway.

©2014 Greenway Health, LLC. All rights reserved. Greenway, the Greenway logo, and PrimeSUITE are registered trademarks or trademarks of Greenway Health, LLC., or its affiliated entities. All other trademarks are the property of their respective owners.

MSO# 19048
5/20/2014

For more information about Greenway, please contact us on the Web at www.greenwayhealth.com

If you have any feedback on this document, or would like to request changes, please send an e-mail to documentationfeedback@greenwayhealth.com. In your message, please include the title and date of the document (listed above) as well as any other information you feel will help with your suggestion.
## Contents

Overview .......................................................... 1
How to Use This Document ........................................ 1
Technical Review .................................................... 2
  Application Architecture ....................................... 3
  Application Security .......................................... 4
  Deployment Models ............................................. 5
    Server Deployment .......................................... 5
    Client Deployment .......................................... 6
PrimeSUITE S+ Hosted Application ................................ 7
Deployment Options ................................................ 9
  Load Balancing ................................................ 9
  Clustering ...................................................... 10
  Virtualization ............................................... 11
  Medical Devices ............................................. 12
  Fax Devices .................................................. 12
  Printers ....................................................... 13
  Scanners ...................................................... 14
Supporting Solutions ............................................... 15
  Clinically-driven Revenue Cycle Management ............. 15
  Application Programming Interface ....................... 15
  Interoperability .............................................. 16
  Enterprise Tasks ............................................. 16
  Dictation ...................................................... 17
  Data Cloud ................................................... 18
  Multi-tenant .................................................. 19
Installation Environment Requirements ............................ 20
  Server and Networking Environment Requirements ........ 20
  Desktop Environment Requirements ......................... 21
  Internet Service Requirements .............................. 24
Installation Management ........................................... 25
Greenway PrimeSUITE 17 System Requirements

Overview

Greenway PrimeSUITE is the leading integrated interoperability solution for Electronic Health Record (EHR) and Practice Management (PM) functionality in medical computing environments of any size. The information in this document is intended for use by Greenway customers, Greenway technicians and other Greenway personnel, and apply to both new installation and upgrade scenarios.

The information in this document applies to PrimeSUITE version 17 and no other version. Refer to the documentation that applies to the version of the application you will be implementing for specific information about that version, as functionality and compatibility may differ.

How to Use This Document

The PrimeSUITE system requirements document is divided into three high-level sections. Each section contains information that applies to all implementations of PrimeSUITE 17 and should be reviewed carefully for both new installation and upgrade implementations.

- **Technical Review** - This section describes the architecture and deployment options available for PrimeSUITE 17, and includes information related to the hosted edition of PrimeSUITE as well as specific security features and installation requirements. Customers who are evaluating a new installation should review this section for information on how best to fit PrimeSUITE into their computing environment.

- **Hardware and Software Requirements** - This section contains specifications and tables that describe the supported servers, workstations and operating systems for a successful implementation of PrimeSUITE. Existing customers who already use a previous version of PrimeSUITE and technicians who are tasked with deployment or technical support should review this section for changes from the previous version.

- **Review Checklist** - In many cases, review of the PrimeSUITE system requirements is a guided process initiated by a Greenway sales or technical representative. Use this checklist to acknowledge acceptance of each high-level requirement and installation option described in this document.
Technical Review

PrimeSUITE has specific architectural and implementation requirements which must be carefully reviewed for all customer computing environments. At a high level, these requirements may be divided into the following topics:

- Application Architecture
- Application Security
- Deployment Models
- PrimeSUITE +S hosted application
- Deployment Options
- Supporting Solutions
- Installation Environment Requirements
- Installation Management

If you are a Greenway customer participating in a guided review of the PrimeSUITE system requirements, refer to the Review Checklist section on page 31 and mark each section appropriately as you review.

If you are not participating in a guided review and need information related to servers, client workstations or operating systems, skip ahead to the Hardware and Software Requirements section on page 27.
Application Architecture

PrimeSUITE may be described as a scalable multilayer web application. Between the end-user and the database, three tiers of application components are deployed:

- **Presentation Layer** - The client components of PrimeSUITE require the use of Microsoft Internet Explorer 8, 9, or 10.
- **Business Logic Layer** - One or more Microsoft Windows servers are deployed to support application and web server functions, and may overlap with the data access layer.
- **Data Access Layer** - One or more Microsoft Windows servers are deployed to support application and web server functions, and may overlap with the business logic layer.

Interoperability, Electronic Health Record (EHR) and Practice Management (PM) components share the same codebase and the store records in a single database. Many competing solutions will typically deploy the EHR and PM components separately, with each function served by a separate application and database. By implementing an integrated solution, PrimeSUITE does not require a dedicated interface engine to coordinate real time workflow or to synchronize redundant database records.

Specific components are used in the development and deployment of PrimeSUITE:

- **Integrated Development Environment (IDE)** - Microsoft Visual Studio (C# and Visual Basic)
- **Software Framework** - Microsoft .NET
- **Web Application Framework** - Microsoft ASP.NET
- **Web Server** - Microsoft Internet Information Services (IIS)
- **Database Server** - Microsoft SQL Server

For information about the specific versions of each component supported for PrimeSUITE 17, refer to the Hardware and Software Requirements section beginning on page 27.
Application Security

To comply with HIPAA regulations, CCHIT certification and other regulatory standards, PrimeSUITE makes use of industry-standard security features intended to safeguard Protected Health Information (PHI) data and to permit detailed auditing of user access. A successful PrimeSUITE login will typically use the following workflow:

Client Security

- The user launches the PrimeSUITE web client.
- The user supplies PrimeSUITE credentials, a unique user name and a password.

Server Security

- The Microsoft Internet Information Services (IIS) web server authenticates the web client request.
- The IIS web server provides access to the PrimeSUITE ASP.NET application resources required for operation of the client program.
- PrimeSUITE ASP.NET application resources authenticate a connection to the Microsoft SQL Server to connect to the PrimeSUITE database.
- PrimeSUITE ASP.NET application resources pass the user credentials supplied previously by the user.
- The user is granted access to PrimeSUITE features and functions for which he or she is authorized or licensed.

This security workflow applies to both thin client and thick client deployment models. Proceed to the next section for a description of these client implementation types.
Deployment Models

This section describes deployment models for PrimeSUITE server systems and client workstations. Read this section carefully to understand deployment model terminology used in other parts of this document.

Server Deployment

PrimeSUITE server systems may be deployed as an inclusive or distributed implementation, depending on the sizing and growth requirements of the customer computing environment.

- **Inclusive Server Deployment** - This type of deployment consolidates all application components, web server components and the Microsoft SQL Server database onto a single server. While an inclusive server may be implemented with external storage or other peripheral devices, all PrimeSUITE components are understood to operate using the same processor and a single Internet Protocol (IP) address.

- **Distributed Server Deployment** - This type of deployment separates the database and the other server components. Typically, the Microsoft SQL Server database will be installed on one server, and the application components and web server components will be installed on a second server.

Server deployment options describe only hardware managed and implemented at the Greenway customer site, or in a datacenter managed by the customer. For information about PrimeSUITE servers that are hosted by Greenway and accessed remotely by Greenway customers, refer to the PrimeSUITE S+ Hosted Application section beginning on page 7.

When deploying PrimeSUITE thin client systems, Microsoft Windows Remote Desktop Services (RDS) is always implemented as a separate server, and is not installed on any server with other application components or database programs.

When deploying virtual machines (VM) guest systems in an environment that supports virtualization, each guest system is understood to be a separate server. An environment that deploys a web server and the database server to separate guest VM systems is described as a distributed deployment, even if both VMs operate on the same host system.

Refer to the Deployment Options section on page 9 for more information on the deployment of VMs in a PrimeSUITE environment.
Client Deployment

PrimeSUITE client systems may be deployed as an as thick client workstations, thin client remote desktops, or a combination of the two.

- **Thick Client** - This is the standard PrimeSUITE client, using a web browser and other program components installed on the local computer workstation. Communication with the server or servers always occurs on the same Local Area Network (LAN). This type of client may also be called the Browser Client in some documentation.

  The Thick Client requires a network connection speed of 300 Kbps per PrimeSUITE session on the local intranet. This requirement excludes other applications, including telephony and Internet browser usage.

- **Thin Client** - The local computer workstation does not have PrimeSUITE program components installed when using the thin client. Instead, a remote connection program is used to connect to a remote desktop where the PrimeSUITE client is already installed. This local program may be Microsoft Remote Desktop Connection (RDC) or the Citrix XenApp Independent Computing Architecture (ICA) client.

  Use of thin clients is recommended when a Greenway customer environment has multiple geographic locations, or when some clients connect to the local network via a Virtual Private Network (VPN). Thin clients may also be used when a workstation does not meet minimum specifications for the PrimeSUITE web browser but is capable of running the RDC program.

  The Thin Client requires an Internet network connection speed of approximately 75 Kbps per RDC session or 35 Kbps per ICA session. This requirement excludes other applications, including telephony and Internet browser usage.

Refer to the Hardware and Software Requirements section for additional information about the supported versions of Microsoft Windows Server and associated Remote Desktop components.
PrimeSUITE S+ Hosted Application

Instead of deploying servers in a Greenway customer computing environment, or in a datacenter managed by the customer, PrimeSUITE may instead be accessed in a hosted environment managed by Greenway in partnership with Dell Services. PrimeSUITE S+ services include dedicated databases, prerequisite software, an integrated backup and upgrade process, and standardized technical support. Additional documentation related to Dell Services datacenter management and service level agreement terms are available by request.

Specific software and hardware requirements listed in this section apply to the PrimeSUITE S+ hosted edition of the program only:

**Localized Technical Support**

- A local certified technical organization or partner company is available to provide initial configuration assistance and ongoing computing environment support.

**Client Machines**

- Desktop, notebook and tablet hardware produced within the last 3 years equipped with a minimum of 4 GB RAM. Hardware specifically intended for use as a thin client device only (such as a Wyse terminal or a Windows Embedded system) are not supported for use as PrimeSUITE S+ clients.
  - Microsoft Windows Vista Business Service Pack 2 (x86/x64) or Microsoft Windows 7 Professional Service Pack 1 (x86/x64).

**Connectivity**

- High speed Internet access to accommodate +/- 75Kbps (upload/download) per Thin Client/RDP session in addition to any bandwidth consumed by general Internet access and other third party software, voice over IP solutions or hardware devices.
  - A hardware-based Virtual Private Network (VPN) IPsec tunnel to each office or practice location with more than five concurrent PrimeSUITE users. This VPN hardware is sold by Greenway for use with PrimeSUITE S+, and requires static IP address blocks to be assigned for successful implementation.
  - A software-based Virtual Private Network (VPN) tunnel from each device located in office or practice locations with fewer than 5 concurrent PrimeSUITE users or located remotely. This VPN software is provided by Greenway for use with PrimeSUITE S+.

**Dictation**

- Philips-brand SpeechMike devices supplied by Greenway, one per dictation user at each Microsoft Windows client workstation.
Faxing
  • One hardware-based fax device per fax line location. This fax hardware is provided by Greenway for use with PrimeSUITE S+.

Medical Devices
  • Midmark and Welch Allyn brand devices, Thin Client compatible.

Printing

Scanning
  • A TWAIN-compliant brand name card or full page scanning device.
  • One RemoteScan (Link) license per physical scanner/scanning workstation supplied by Greenway.
Deployment Options

To facilitate high availability and maximize the usage of computing resources, PrimeSUITE supports a number of industry-standard deployment options and support for peripherals. The following topics are described in this section:

- Load balancing
- Clustering
- Virtualization
- Medical Devices
- Fax Devices
- Printers
- Scanners

Load Balancing

Load balancing refers to the redirection of network traffic to multiple and redundant systems. Although a user perceives only one back-end web site or database, two or more servers are used to distribute the load of client connections, and to ensure availability in the unlikely event of hardware failure or network failure. Specific to PrimeSUITE, hardware load balancing may be used to accelerate and distribute traffic directed to multiple web servers in a distributed server deployment.

This type of load balancing is typically implemented and supported by individual hardware vendors, and configuration may differ depending on the brand or type of servers that are installed. For this reason, Greenway does not provide technical support or configuration instructions for hardware load balancing.

For detailed information on hardware load balancing, refer to vendor documentation for your specific server hardware.
Clustering

Microsoft SQL Server provides the capability to distribute software functions among two or more servers. Specifically, failover clustering is used to ensure high availability and redundancy, by replicating data between two or more database servers. For detailed information on configuration and setup of Microsoft SQL Server clustering, refer to the Microsoft documentation at the following URL:


Clustering is supported only for distributed server deployment. Inclusive server deployment will necessarily implement only one Microsoft SQL Server database, and clustering does not also replicate application or web server components.

The following illustration depicts one example of PrimeSUITE deployed to use Microsoft SQL Server failover clustering, with multiple database servers and a large external disk array.
Virtualization

Specifications and requirements listed for PrimeSUITE server components refer to physical server hardware only. However, in a distributed server deployment Greenway customers may elect to implement application servers or web servers as virtual machine (VM) devices.

A virtual server is a complete computing system implemented as software only. Hardware such as the CPU, memory, and network interface are emulated in software. The advantages of implementing a virtual server include operation of multiple virtual servers on a single host device, and the ability to move a virtual server to a backup device or to another host. Greenway provides support for implementation of virtual servers on industry-standard host systems such as VMWare ESX, Microsoft Hyper-V and Citrix XenServer.

Greenway strongly recommends that database servers be implemented as physical hardware only, and not as virtual machines.

Note the following restrictions and additional requirements when implementing virtual servers in a PrimeSUITE environment:

• When specifying virtual hardware components for each VM, configure settings to match or exceed the requirements for a physical server. Refer to the Hardware and Software Requirements section on page 27 for a comprehensive list of specifications.

• At a minimum, virtual application and web servers must be configured to use four virtual CPUs. This requirement supersedes other specifications.

• At a minimum, virtual remote desktop servers require two virtual CPUs to be configured.

• Greenway strongly recommends that database servers be implemented as physical hardware only. When implementing a virtual database server, a minimum of four virtual CPUs must be configured.

• As a best practice, the Intel Hyperthreading CPU feature must be disabled both on the host system and on each configured guest system when Intel CPUs prior to the Nehalem hardware revision are in use. When configured incorrectly, technicians and support personnel may observe high processor usage from the sqlservr.exe application process.

Refer to the vendor documentation for the specific virtualization solution in your environment for additional information regarding VMWare, Citrix or Microsoft Hyper-V virtual machine implementation.
Medical Devices

PrimeSUITE is engineered to connect to many leading diagnostic and vitals data devices. Stationary electrocardiography or mobile Holter, spirometry, stress and vitals information may be entered into the PrimeSUITE database using a compatible device. Contact a Greenway sales representative for specific information regarding supported manufacturers, and compatible devices and models.

Fax Devices

PrimeSUITE natively supports the use of the EHRfax MultiTech FaxFinder device, and may be configured to use other standard fax devices such as the OpenText RightFax solution.

Greenway provides sales and support for the EHRfax MultiTech FaxFinder device. For additional information on this hardware, refer to the vendor documentation at the following URLs:

http://multitech.com/
http://www.ehrtools.com/index.php?option=com_content&view=article&id=115&Itemid=113

The following illustration depicts one example of a successfully implemented fax solution for a PrimeSUITE environment. Contact a Greenway sales representative for additional information on sizing and configuration of an appropriate fax solution.
Printers

PrimeSUITE is coded to use standard printer calls and functions already present in Microsoft Windows. These functions include locally-installed printers, shared network printers and the Easy Print function of Remote Desktop Services. Easy Print provides distributed printer access without the installation of drivers. For detailed information on Easy Print refer to the Microsoft documentation at the following URL:


The following illustration depicts one example of a distributed printer configuration at a PrimeSUITE customer site, which includes local printers and shared network printers.
Scanners

PrimeSUITE supports devices used to scan full-page documents or smaller card documents, in both the Thin Client and Thick Client deployment models. Scanning for thin clients requires the implementation of the RemoteScan product, to provide connectivity through the existing remote desktop client.

For detailed information on the RemoteScan product, refer to the vendor documentation at the following URL:

http://www.remote-scan.com/

The following illustrate depicts two examples of successful scanner device implementation in a PrimeSUITE environment.
Supporting Solutions

Greenway provides many additional services and software programs designed to enhance and expand the functionality of PrimeSUITE. These functions are collectively known as Supporting Solutions and are divided into the following categories:

• Clinically-driven Revenue Cycle Management
• Application Programming Interface
• Interoperability
• Enterprise Tasks
• Dictation
• Data Cloud
• Multi-tenant

Clinically-driven Revenue Cycle Management

PrimeSUITE includes clinically-drive revenue cycle management (RCM) capabilities via the PrimeRCM product. A team of billing experts drives a cloud-based software-as-a-service (SaaS) platform to provide RCM functionality without additional technical infrastructure. PrimeRCM may be used for both on-premise and hosted PrimeSUITE S+ customers.

For additional information regarding PrimeRCM, refer to the following URL:

http://www.greenwaymedical.com/solutions/primercm/

Application Programming Interface

The core PrimeSUITE EHR and PM solution may be extended with additional functionality offered by Greenway partners at the Greenway Marketplace website. An application programming interface (API) is available to Greenway partners to make additional functionality available outside of the core product. Greenway customers and Greenway partners are encouraged to participate in the Marketplace program to share ideas and resolve unique workflow challenges. Access the Greenway Marketplace at the following URL:

http://marketplace.greenwaymedical.com/
Interoperability

PrimeSUITE enables data exchange through the PrimeEXCHANGE service. A centralized interoperability engine is hosted and managed by Greenway, and unlike competing services it is not installed or implemented at a customer site.

For detailed information regarding the PrimeEXCHANGE service refer to the following URL: http://www.greenwaymedical.com/solutions/prime-exchange/

Enterprise Tasks

PrimeSUITE enables enterprise-level business process management to administer multiple practices and large medical businesses. Dedicated enterprise business logic is accessed through a dedicated server, or a separate application/web server connected to the database.
Dictation

PrimeSUITE supports dictation and transcription functionality in both the thick client and thin client deployment models, through the PrimeSPEECH product offering. Dictation requests are transmitted to a central system administered by Greenway, and securely returned to the PrimeSUITE database as text.

Note that implementation of PrimeSPEECH increases the memory usage of client components. Specifically, a PrimeSUITE user who is assigned a PrimeSPEECH author ID and has enabled the speech capabilities will use four times as much memory per client process than a PrimeSUITE client without PrimeSPEECH enabled.

For additional information regarding the PrimeSPEECH solution, refer to the information at the following URL:

Data Cloud

A number of PrimeSUITE features related to research and analysis are housed in the Greenway Data Cloud, an Internet-hosted repository of capabilities intended to expand and to enhance the functionality of any PrimeSUITE implementation. A number of secure connectors and services are available.

Secure Connectors

- Continuity of Care Document (CCD) transmission
- Longitudinal Continuity of Care Document (LCCD) transmission
- Nationwide Health Information Network (NHIN) CONNECT gateway
- Customized connectors for other third-parties

Services

- Accountable Care Organization (ACO) services
- Clinical Decision Support (CDS) alerts
- Business Intelligence (BI) analysis and management
- Center for Medicare & Medicaid Services (CMS) Physician Quality Reporting System (PQRS) incentive
- CMS ePrescribe (eRx) incentive
- Community Document viewing
- Meaningful Use (MU) monitoring
- Messaging
Multi-tenant

PrimeSUITE may be implemented to support multiple tenants. In this type of implementation, one database server is configured to house multiple database instances, each of which is configured to connect to a separate application and web server. Each database may therefore support a separate practice, or even different Greenway customers. A multi-tenant implementation may optionally use Microsoft SQL Server failover clustering or a Storage Area Network (SAN) disk array.

Observe that different versions of PrimeSUITE may be installed concurrently on a database server implemented for a multi-tenant environment.
Installation Environment Requirements

Any implementation of PrimeSUITE has specific environmental requirements to ensure the health and proper ongoing operation of servers, workstations, and other elements of the computing environment. On-site implementations that include servers, and any environment with network hardware should conform to the requirements listed below for server and networking environment requirements. All installations that include desktop workstations should conform to the desktop environment requirements listed below. All environments must also conform to the Internet Services Requirements listed.

Server and Networking Environment Requirements

Servers implemented in a PrimeSUITE installation have general requirements related to cooling, power, and access security.

- **Cooling** - Manufacturers of server and networking equipment will specify ideal ranges for operating temperature, storage temperature and humidity. To optimize performance and achieve the maximum operating lifespan of these types of devices, maintain an appropriate level of cooling and dehumidifying wherever servers are installed.

  Contact a Greenway sales representative for specific technical information regarding the cooling needs of any hardware supplied by Greenway.

- **Power** - All server and network devices should be installed in a dedicated area with the proper configuration and sizing of electrical power. Specifically, Uninterruptible Power Supply (UPS) devices must be installed to provide continuous power during an unplanned or intermittent power failure, or to permit administrative action such as a managed shutdown.

  Contact a Greenway sales representative for specific technical information regarding the power requirements of any hardware supplied by Greenway.

- **Security** - When implementing servers and network equipment on-site, access must be restricted to authorized persons. The dedicated area where servers and network devices are installed should be properly locked and secured against intrusion or other unauthorized physical access.

- **Wired and Wireless Networking** - As a best practice, install and test wired network media before installing servers and network devices. When implementing a wireless network, make use of industry standards for wireless encryption, configuration and testing. When installing wireless access points, locate these devices in areas where wireless client systems are most likely to be used.

  Observe that wireless interference may occur in computing environments that include some medical devices, such as imaging equipment.

- **Internet for Remote Connectivity** - A full-time Internet connection is required for all PrimeSUITE installations to support remote connectivity features used by Greenway Application and Technical Support. A dedicated Virtual Private Network (VPN) tunnel is implemented using a specialized firewall device supplied by Greenway. A minimum upload and download bandwidth speed of 384 Kbps is required to support the VPN connection.
Contact a Greenway sales representative for specific technical information regarding network equipment supplied by Greenway.

**Desktop Environment Requirements**

Microsoft Windows client workstations implemented in a PrimeSUITE environment require specific web browser settings for correct operation. When configuring the web browser, other settings related to web content filtering and Citrix client applications must also be configured. Use the information in this section to configure or troubleshoot client workstation operation.

- **Web Browser Settings** - PrimeSUITE client operation is dependent on the correct configuration of Internet Explorer. Specifically, the Trusted Sites and Zone Security Level Settings must be correctly configured. Instead of configuring individual client workstations, as a best practice use a Microsoft Windows local or domain-based computer policy to configure all clients in your environment at the same time.

On the Microsoft Windows domain controller, or on the stand-alone Remote Desktop Services server, open the Local Group Policy Editor from the graphical user interface or with the command line instruction ‘gedit.msc’.

At the top level, two sets of policies are available, labeled Computer Configuration and User Configuration. Expand the Computer Configuration policy set and browse through the following folders:

- Administrative Templates -> Windows Components -> Internet Explorer ->
- Internet Control Panel -> Security Page
In the Security Page folder open the Properties of the ‘Site to Zone Assignment List’ setting. Enable this setting and click the Show button to configure zone assignments.

Add a zone assignment for each application and web server in your PrimeSUITE environment, using the URL as the Value Name and the numeral ‘2’ for each value. For example, for a server with the NetBIOS name ‘ApplicationWeb01’ enter the URL in the Value Name column as ‘http://ApplicationWeb01’.

After configuring the Site to Zone Assignment List return to the Security Page folder and open the ‘Trusted Sites Zone’ folder. Observe that several settings are available to be enabled or disabled as needed.

Enable the following settings:

- Allow Scriptlets
- Automatic Prompting for ActiveX controls
- Download signed ActiveX controls
- Download unsigned ActiveX controls
- Initialize and script ActiveX controls not marked as safe

For detailed information on the usage of the Local Group Policy Editor for all supported versions of Microsoft Windows, refer to the Microsoft Technet documentation at the following URL:

• Web content filtering and proxy server configuration - Many Greenway customer computing environments may include web content filtering or web browser proxy systems, to ensure security and appropriate business usage of client workstations. To support the correct operation of PrimeSUITE and other Internet-based applications, HTTP web traffic used for PrimeSUITE communication must not be blocked or redirected by these systems.

When configuring web content filtering, all application and web server URLs must be configured as trusted domains. When configuring the proxy server functionality of Internet Explorer, exclude application and web server URLs by adding these addresses to the Proxy Server Exception list.

• Citrix XenApp configuration - PrimeSUITE client applications may be used with the Citrix XenApp remote connectivity client. However, an additional configuration step must be completed for all Microsoft Windows desktops using the PrimeSUITE client as a published application, to support Microsoft Windows user profile settings not present in the Citrix shell. Refer to the Citrix knowledge base article CTX127874 at the following URL:

http://support.citrix.com/article/CTX127874

Some peripheral functionality may also be affected, such as the EHRfax MultiTech FaxFinder device. A number of software drivers may not operate correctly with Citrix XenApp published applications without additional configuration. Contact a Greenway application or technical support representative for assistance with the configuration of fax devices with Citrix XenApp.
Internet Service Requirements

Connectivity to third-party web services located on the Internet is required for successful operation of many PrimeSUITE features and functions. All clients, servers, and network devices that are part of a PrimeSUITE installation must have open access to the following IP addresses and TCP ports.

<table>
<thead>
<tr>
<th>Web Service Usage</th>
<th>Numeric IP Address</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claims, Electronic Remittance Advice (ERA) and Batch Eligibility</td>
<td>143.112.40.23</td>
<td>SFTP (Secure File Transfer Protocol)</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>204.138.99.81</td>
<td>SFTP</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>65.57.254.50</td>
<td>SFTP</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>69.2.197.40</td>
<td>SFTP</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>208.79.134.63</td>
<td>SFTP</td>
<td>22</td>
</tr>
<tr>
<td>Claims and ERA</td>
<td>205.216.7.14</td>
<td>SFTP</td>
<td>9922</td>
</tr>
<tr>
<td></td>
<td>216.104.80.185</td>
<td>SFTP</td>
<td>22</td>
</tr>
<tr>
<td>Claims</td>
<td>74.63.172.37</td>
<td>SFTP</td>
<td>22</td>
</tr>
<tr>
<td>Statements</td>
<td>208.86.15.54</td>
<td>SFTP</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>216.161.200.38</td>
<td>SFTP</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>209.90.66.3</td>
<td>SFTP</td>
<td>22</td>
</tr>
<tr>
<td>Real-time Eligibility</td>
<td>143.112.40.27</td>
<td>SSL (Secure Sockets Layer)</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>204.138.99.77</td>
<td>SSL</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>64.57.254.44</td>
<td>SSL</td>
<td>7000</td>
</tr>
<tr>
<td></td>
<td>69.2.197.41</td>
<td>SSL</td>
<td>443</td>
</tr>
<tr>
<td>Orders</td>
<td>170.138.220.93</td>
<td>SSL</td>
<td>443</td>
</tr>
<tr>
<td>ePrescribe</td>
<td>65.221.4.67</td>
<td>SSL</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>65.221.4.102</td>
<td>SSL</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>65.221.4.103</td>
<td>SSL</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>65.221.4.104</td>
<td>SSL</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>65.221.4.107</td>
<td>SSL</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>65.221.4.211</td>
<td>SSL</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>65.221.4.216</td>
<td>SSL</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>65.221.4.229</td>
<td>SSL</td>
<td>443</td>
</tr>
<tr>
<td>Dictation</td>
<td>66.45.73.253</td>
<td>SSL</td>
<td>443</td>
</tr>
</tbody>
</table>

Addresses and connectivity requirements may change without notice. Contact a Greenway application or technical support representative if you need assistance with configuration or troubleshooting of these services.
Installation Management

A number of computing environment functions are not unique to PrimeSUITE but should be present to ensure availability and continuity of operation.

• Backups - All PrimeSUITE computing environments are required to use application and database backup systems. In addition to disk-based backups configured for Microsoft SQL Server, system-level backup software must be implemented to protect the operating system and other related system state data. Both tape and disk backup media may be used.

Symantec Backup Exec or another industry-standard backup solution should be implemented for all servers in a PrimeSUITE environment. When available, a specific agent for database backups must also be installed. As a best practice, to prevent data loss due to fire, flood, or other disaster scenario which might destroy a tape or a removable drive, at least one backup media item must be periodically moved off-site for maximum security. As a best practice, test recovery from backup media once per quarterly interval.

• Microsoft Update - All servers should be configured to use the Microsoft Update service for operating system, database platform and other supported application updates. Critical updates related to security and stability should be installed as they become available.

Greenway regularly tests and certifies service packs, and other major updates to compatible operating system and database platforms. Contact a Greenway application or technical support representative before installing a service pack or other major update to ensure continuous operation of your PrimeSUITE system.
• Malware protection - All PrimeSUITE computing environments are required to include industry-standard virus and spyware protection software. To optimize performance of inclusive servers and database servers, configure this software to exclude Microsoft SQL Server files from real-time scanning. These files will have the following file extensions:
  *.mdf
  *.ldf

• Performance Monitoring- A combination of Microsoft Windows tools and third-party solutions may be used to monitor the performance and efficiency of the PrimeSUITE environment. Greenway customers and technicians may use any of the tools listed in this section.

<table>
<thead>
<tr>
<th>Monitoring Tool Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built-in tools for clients and servers</td>
<td>Microsoft Windows Task Manager</td>
</tr>
<tr>
<td>Built-in tools for servers</td>
<td>Microsoft Windows Task Manager</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Performance Monitor</td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server Profiler</td>
</tr>
<tr>
<td>Downloadable tools</td>
<td>Microsoft Sysinternals</td>
</tr>
<tr>
<td></td>
<td>Process Monitor</td>
</tr>
<tr>
<td></td>
<td>Process Explorer</td>
</tr>
<tr>
<td></td>
<td>Fiddler Web Debugger</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.fiddler2.com/fiddler2/">http://www.fiddler2.com/fiddler2/</a></td>
</tr>
</tbody>
</table>

• Security - Access to Protected Health Information (PHI) is restricted to authorized PrimeSUITE users via built-in application security. All access to PHI from outside the PrimeSUITE application must be carefully assigned to administrators, analysts and end users. Direct access to servers should be limited to administrative users only. Microsoft password policies should be used to enforce password history variables, and to set age, length, and complexity requirements.

PrimeSUITE supports the use of Secure Socket Layer (SSL) certificates at the Application/Web server level to secure HTTP communications.

PrimeSUITE supports the use of Microsoft Active Directory integration to institute single sign-on capabilities.

Encryption of sensitive data for each PrimeSUITE practice database may be applied using the Transparent Data Encryption feature of Microsoft Windows:

Hardware and Software Requirements

PrimeSUITE implementations support many different configurations depending on the size of the environment and the number of user connections that are supported. Use the information in this section to guide purchasing and configuration of the appropriate type of servers and workstations for your environment.

If you are a Greenway customer participating in a guided review of the PrimeSUITE system requirements, refer to the Review Checklist section on page 31 and mark each section appropriately as you review.

If you are not participating in a guided review and need information related to architecture and environmental requirements, return to the Technical Review section beginning on page 2.

Minimum Server Requirements

Use this chart to guide purchasing and configuration of server hardware based on the number of users in your environment and the type of server deployment in use. Refer to the Deployment Models section on page 5 for an explanation of inclusive and distributed server deployment models.

Inclusive Server Deployment systems:

<table>
<thead>
<tr>
<th>User Sessions</th>
<th>Server Type</th>
<th>Minimum CPU</th>
<th>Minimum RAM</th>
<th>Disk and RAID requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-10 users</td>
<td>Application/Web and Database</td>
<td>1 Intel Xeon, 6 cores</td>
<td>16 GB</td>
<td>(5) 300 GB 15K RPM (4) Disk RAID 10 with 1 Global Spare</td>
</tr>
<tr>
<td>11-99 users</td>
<td>Application/Web and Database</td>
<td>1 Intel Xeon, 8 cores</td>
<td>32 GB</td>
<td>(5) 600 GB 15K RPM (4) Disk RAID 10 with 1 Global Spare</td>
</tr>
</tbody>
</table>
### Distributed Server Deployment systems:

<table>
<thead>
<tr>
<th>User Sessions</th>
<th>Server Type</th>
<th>Minimum CPU</th>
<th>Minimum RAM</th>
<th>Disk and RAID requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 users per server</td>
<td>Application/Web</td>
<td>1 Intel Xeon, 8 cores</td>
<td>16 GB</td>
<td>(3) 300 GB 15K RPM (2) Disk RAID 1 with 1 Global Spare</td>
</tr>
<tr>
<td>100-250 users</td>
<td>Database</td>
<td>1 Intel Xeon, 8 cores</td>
<td>32 GB</td>
<td>(9) 600 GB 15K RPM (8) Disk RAID 10 with 1 Global Spare</td>
</tr>
<tr>
<td>251-600 users</td>
<td>Database</td>
<td>2 Intel Xeon, 8 cores</td>
<td>48 GB</td>
<td>(9) 600 GB 15K RPM (2) Disk RAID 1 (6) Disk RAID 10 with 1 Global Spare</td>
</tr>
<tr>
<td>600-1,000 users</td>
<td>Database</td>
<td>2 Intel Xeon, 8 cores</td>
<td>48 GB</td>
<td>(11) 600 GB 15K RPM (2) Disk RAID 1 (2) Disk RAID 1 (6) Disk RAID 10 with 1 Global Spare</td>
</tr>
<tr>
<td>1,001-2,500 users</td>
<td>Database</td>
<td>4 Intel Xeon, 8 cores</td>
<td>64 GB</td>
<td>(11) 600 GB 15K RPM (2) Disk RAID 1 (2) Disk RAID 1 (6) Disk RAID 10 with 1 Global Spare</td>
</tr>
</tbody>
</table>

### Other Server Deployment systems:

<table>
<thead>
<tr>
<th>User Sessions</th>
<th>Server Type</th>
<th>Minimum CPU</th>
<th>Minimum RAM</th>
<th>Disk and RAID requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise (user count N/A)</td>
<td>Application/Web and Database</td>
<td>1 Intel Xeon, 8 cores</td>
<td>32 GB</td>
<td>(5) 600 GB 15K RPM (4) Disk RAID 10 with 1 Global Spare</td>
</tr>
<tr>
<td>1-50 Remote Desktop sessions</td>
<td>Remote Desktop Services client server</td>
<td>1 Intel Xeon, 8 cores</td>
<td>16 GB</td>
<td>(3) 300 GB 15K RPM (2) Disk RAID 1 with 1 Global Spare</td>
</tr>
</tbody>
</table>

Note the following server configuration requirements, which apply to all servers regardless of deployment or sizing:

- Optical DVD-R drive required.
- Redundant power supply required.
- Two Gigabit ethernet connections required.
- A Remote Management Adapter is required.
- Removable disk cartridge or tape drive backup device is required (except for Remote Desktop servers and distributed Application/Web servers)
Minimum Client Workstation Requirements

Use this chart to guide purchasing and configuration of client workstation hardware based on the type of hardware required.

**Client Workstation systems:**

<table>
<thead>
<tr>
<th>Workstation hardware</th>
<th>Minimum CPU</th>
<th>Minimum RAM</th>
<th>Minimum Disk</th>
<th>Required network connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop</td>
<td>1 Intel Core 2 Duo Dual Core</td>
<td>4 GB</td>
<td>320 GB</td>
<td>1 Gigabit Ethernet</td>
</tr>
<tr>
<td>Notebook/Laptop</td>
<td>1 Intel Core i5 Dual Core</td>
<td>4 GB</td>
<td>320 GB</td>
<td>1 Gigabit Ethernet 1 Wireless 802.11 b/g/n</td>
</tr>
<tr>
<td>Tablet</td>
<td>1 Intel Core i5 Dual Core</td>
<td>4 GB</td>
<td>320 GB</td>
<td>1 Gigabit Ethernet 1 Wireless 802.11 b/g/n</td>
</tr>
</tbody>
</table>

Workstation specifications apply to all client implementations, including thick client, thin client and Citrix XenApp implementations.

**Software**

Different server and client deployment models may support different versions or editions of operating systems, database products or web browsers. Refer to the specific section for the type of device for the appropriate information.

**Servers**

Some software is present on specific types of servers only. For example, in a distributed deployment an application and web server may not also include a database server.

**Application/Web Server**

Microsoft Windows Server 2008 R2 Standard Edition, 64-bit only

**Database Server**

Microsoft Windows Server 2008 R2 Standard Edition, 64-bit only, or
Microsoft Windows Server 2008 R2 Enterprise Edition, 64-bit only

Microsoft SQL Server 2008 R2 Standard Edition, or
Microsoft SQL Server 2008 R2 Enterprise Edition

**Remote Desktop Services Server**

Microsoft Windows Server 2008 R2 Standard Edition, 64-bit only, or
Microsoft Windows Server 2008 R2 Enterprise Edition, 64-bit only

Microsoft Internet Explorer 8.0, Internet Explorer 9.0, or Internet Explorer 10.0
Adobe Acrobat Reader XI (required for use of PrimeRCM supporting solution)
**Clients**

Client software requirements differ between thin client and thick client implementations.

**Thick Client (Browser Client)**

- Microsoft Windows Vista Business SP2, 32-bit or 64-bit
- Microsoft Windows 7 Professional SP1, 32-bit or 64-bit
- Microsoft Windows 8 Professional, 32-bit or 64-bit
- Microsoft Internet Explorer 8.0, Internet Explorer 9.0, or Internet Explorer 10.0
- Adobe Acrobat Reader XI (required for use of PrimeRCM supporting solution)

**Thin Client (Browser Client)**

- Microsoft Windows Vista Business SP2, 32-bit or 64-bit or
- Microsoft Windows 7 Professional SP1, 32-bit or 64-bit or
- Microsoft Windows 8 Professional, 32-bit or 64-bit
- Wyse ThinOS
- Microsoft Windows CE
- Linux
- Microsoft Windows Embedded Standard 2009
- Microsoft Windows Embedded Standard 7

Note that vendor support for all editions of Microsoft Windows XP will end in April 2014. Greenway products released after April 2014 will not be permitted to be installed or run on Microsoft Windows XP. Greenway strongly recommends that PrimeSUITE customers migrate or upgrade existing client systems whenever possible to maintain secure standards and regulatory compliance.

**Portable Devices**

PrimeMOBILE is the PrimeSUITE client application for portable systems, and may be implemented on compatible tablet or handheld computing devices. However, specific hardware requirements may change as application updates are applied. For each portable device, refer to the appropriate vendor application website for specific information regarding PrimeMOBILE hardware requirements and prerequisites.

- **Apple iOS:**
  

- **Google Android:**
  

- **Microsoft Windows 8:**
  

Note that compatibility with Microsoft Windows 8 RT is specific to the PrimeMOBILE application only. Refer to the previous section for client workstation requirements that apply to the standard thick client and thin client implementations of PrimeSUITE.
Review Checklist

In many cases, review of the PrimeSUITE system requirements is a process guided by a Greenway sales or technical representative. Use this checklist to acknowledge acceptance of each high-level requirement and installation option described in this document.

Greenway Responsibilities

Greenway is dedicated to the success of every PrimeSUITE installation. This dedication applies to both installation models, the turn-key model with hardware and software supplied by Greenway, and the remote model with only software supplied by Greenway. This document services as a guide of requirements and best practices for this information.

Client Responsibilities

Prior to configuration or staging of an appropriate-sized environment, a successful installation of PrimeSUITE requires a thorough understanding and acknowledgement of the topics included in this document. As a Greenway representative guides you through these topics, please make a checkmark and add your initials to each section and subsection, and sign at the bottom of the form to acknowledge your review and understanding.

<table>
<thead>
<tr>
<th>Check</th>
<th>Check</th>
<th>Initial</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Application Architecture, page 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Application Security, page 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Deployment Models, page 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Server Deployment, page 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Client Deployment, page 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PrimeSUITE S+ Hosted Application, page 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Deployment Options, page 9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Load Balancing, page 9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Clustering, page 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Virtualization, page 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Medical Devices, page 12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fax Devices, page 12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Printers, page 13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Scanners, page 14</td>
</tr>
<tr>
<td>Check</td>
<td>Check</td>
<td>Initial</td>
<td>Topic</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Supporting Solutions, page 15</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Clinically-driven Revenue Cycle Management, page 15</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Application Programming Interface, page 15</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Interoperability, page 16</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Enterprise Tasks, page 16</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Dictation, page 17</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Data Cloud, page 18</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Multi-tenant, page 19</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Installation Environment Requirements, page 20</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Server and Networking Environment Requirements, page 20</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Cooling, page 20</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Power, page 20</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Security, page 20</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Wired and Wireless Networking, page 20</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Internet for Remote Connectivity, page 20</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Desktop Environment Requirements, page 21</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Internet Service Requirements, page 24</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Installation Management, page 25</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Backups, page 25</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Microsoft Update, page 25</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Malware Protection, page 25</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Performance Monitoring, page 25</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Security, page 25</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Hardware and Software Requirements, page 27</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Client and Server Hardware, pages 28-30</td>
</tr>
<tr>
<td>🗙</td>
<td></td>
<td></td>
<td>Client and Server Software, pages 28-30</td>
</tr>
</tbody>
</table>

BY (company name):

(Date)

(Authorized Signature)

(Typed or Printed Name)

(Title)