

Greenway Prime Suite / Version 18.30

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.

© 2021 Greenway Health, LLC. All rights reserved. Greenway, the Greenway logo, and Prime Suite are registered trademarks or trademarks of Greenway Health, LLC., or its affiliated entities. All other trademarks are the property of their respective owners.

Last Modified: 10/13/2021

MSO #21719

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

To provide feedback or request changes to a document, send an e-mail to documentationfeedback@greenwayhealth.com. In your message, be sure to include the title and date of the document (listed above).

Reporting Patient Safety, HIPAA, or Regulatory Concerns

To report patient safety, HIPAA, or regulatory concerns, or for any other product concerns, [chat with us](#) or [add a support case](#) via [My Greenway \(greenwayhealth.force.com\)](https://greenwayhealth.force.com), or call us at (877) 932-6301, opt. 2

4301 W. Boy Scout Blvd
Ste. 800
Tampa, FL 33607
877-932-6301

www.greenwayhealth.com



Table of Contents

In Brief.....	6
How to Use This Document	7
Technical Review	8
Application Architecture.....	9
Application Security.....	10
On Communications Between Client and Server	11
Deployment Models.....	12
Server Deployment	12
Client Deployment	13
Prime Suite+S Hosted Application	15
Localized Technical Support	15
Client Machines.....	15
Connectivity	15
Dictation.....	15
Faxing.....	16
Medical Devices	16
Printing.....	16
Scanning	16
Deployment Options	17
Load Balancing.....	17
Clustering.....	18
Virtualization.....	19
Medical Devices	20
Fax Devices.....	20
Printers.....	21
Scanners	22
Supporting Solutions	23
Clinically-driven Revenue Cycle Management	23
Application Programming Interface.....	23
Interoperability.....	23
Dictation.....	24
Data Cloud	25
Multi-tenant.....	26
Installation Environment Requirements.....	27
Server and Networking Environment Requirements.....	27
Desktop Environment Requirements	28
Web Browser Settings	28
Web Content Filtering and Proxy Server Configuration	30
Citrix XenApp Configuration	31

Internet Service Requirements	31
Installation Management	33
Back Ups	33
Microsoft Update	33
Malware Protection.....	34
Performance Monitoring.....	35
Security	35
Hardware and Software Requirements.....	36
Minimum Server Requirements.....	36
Minimum Client Workstation Requirements	38
Software.....	38
<i>Setup Requirements</i>	38
<i>Servers</i>	39
<i>Clients</i>	40
<i>Portable Devices</i>	40
Review Checklist.....	41
Greenway Responsibilities.....	41
Client Responsibilities.....	41

Changelog

Date	Change Description
10/13/2020	<ul style="list-style-type: none">• Added notes regarding the types of storage device that can be used under the Minimum Server Requirements section.• Updated the information related to Prime Suite support for clustering, fax device, printer, and scanner under the Deployment Options section.

In Brief

Greenway Prime Suite 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 Prime Suite version 18.30 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 Prime Suite system requirements document is divided into three high-level sections. Each section contains information that applies to all implementations of Prime Suite 18.00 and should be reviewed carefully for both new installation and upgrade implementations.

- **Technical Review** - This section describes the architecture and deployment options available for Prime Suite 18.00, and includes information related to the hosted edition of Prime Suite 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 Prime Suite 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 Prime Suite. Existing customers who already use a previous version of Prime Suite 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 Prime Suite 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

Prime Suite 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
- Prime Suite+S hosted application
- Deployment Options
- Supporting Solutions
- Installation Environment Requirements
- Installation Management

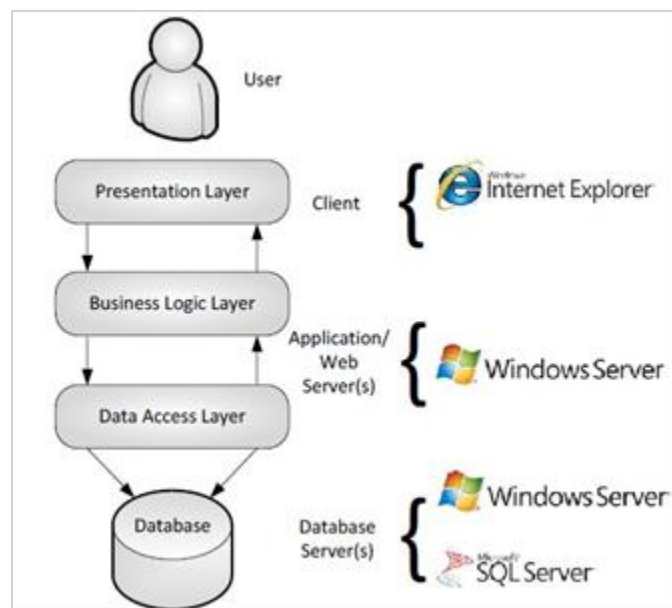
If you are a Greenway customer participating in a guided review of the Prime Suite system requirements, refer to the [Review Checklist](#) section on page 39 and mark each section appropriately as you review.

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 34.

Application Architecture

Prime Suite 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 Prime Suite require the use of Microsoft Internet Explorer 11.
- 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, Prime Suite 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 Prime Suite:

- 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 Prime Suite 18.00, refer to the [Hardware and Software Requirements](#) section beginning on page 34.

Application Security

To comply with HIPAA regulations, CCHIT certification and other regulatory standards, Prime Suite makes use of industry-standard security features intended to safeguard Protected Health Information (PHI) data and to permit detailed auditing of user access.

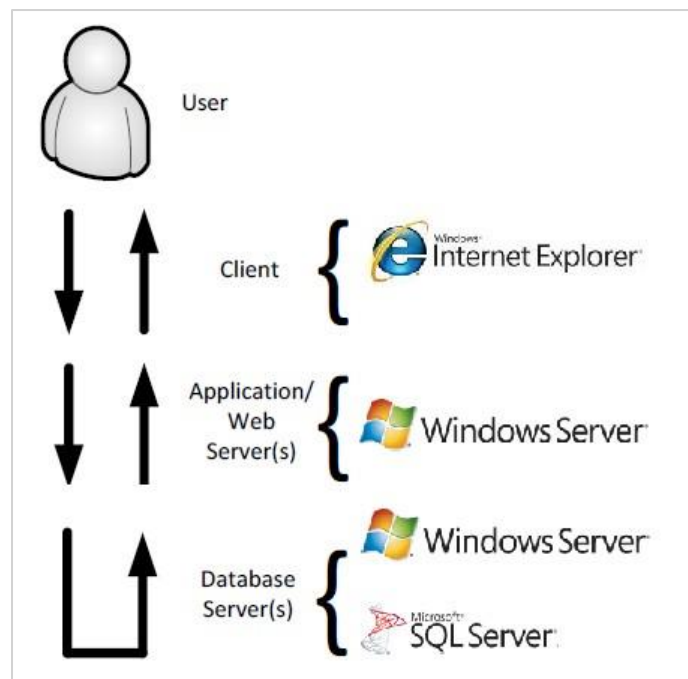
A successful Prime Suite login will typically use the following workflow:

Client Security

- The user launches the Prime Suite web client.
- The user supplies Prime Suite 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 Prime Suite ASP.NET application resources required for operation of the client program.
- Prime Suite ASP.NET application resources authenticate a connection to the Microsoft SQL Server to connect to the Prime Suite database.
- Prime Suite ASP.NET application resources pass the user credentials supplied previously by the user.
- The user is granted access to Prime Suite 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.

On Communications Between Client and Server

Greenway Prime Suite is currently designed to run on private networks. Web (http) traffic between the Client/Browser (i.e. Microsoft Internet Explorer, or IE) and Web Server (i.e. Microsoft Internet Information Services, or IIS) is unencrypted. However, customers may choose to introduce the use of a Secure Sockets Layer (SSL) certificate to encrypt that web traffic.

All communications between the platform's Application/Web Server(s) and Database Server is also currently unencrypted. All data, outside of user passwords, located within the solution's designated Microsoft SQL Server databases is unencrypted. Customers may choose to introduce the use of hardware disk encryption and/or Microsoft SQL Server Enterprise Edition Transparent Data Encryption (TDE) to encrypt Electronic Health Protected Information (ePHI). They may also choose to introduce the use of Microsoft SQL Server encrypted complete and transaction log backups.

In public Internet based deployments, private Local Area Networks (LANs) and Wide Area Networks (WANs), current standards employ the use of Microsoft Remote Desktop Services with or without Citrix XenApp. Both of these include encryption with their respective Remote Desktop Protocol (RDP) and Independent Computing Architecture (ICA) Thin Client communication protocols.

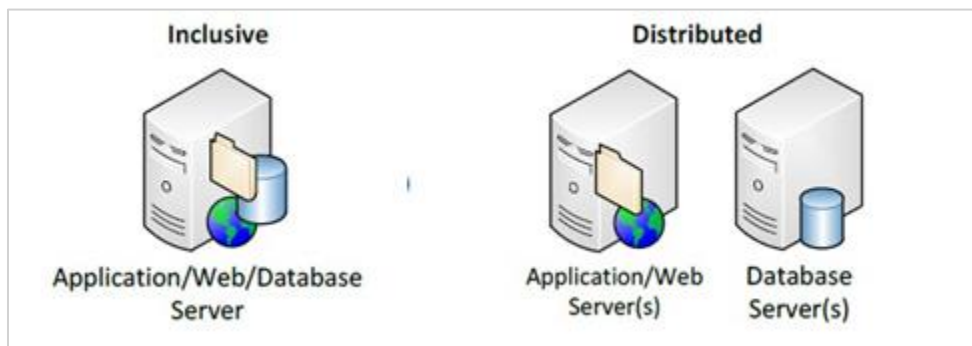
Deployment Models

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

Server Deployment

Prime Suite 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 Prime Suite 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 Prime Suite servers that are hosted by Greenway and accessed remotely by Greenway customers, refer to the [Prime Suite S+ Hosted Application](#) section beginning on page 7.

When deploying Prime Suite 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.

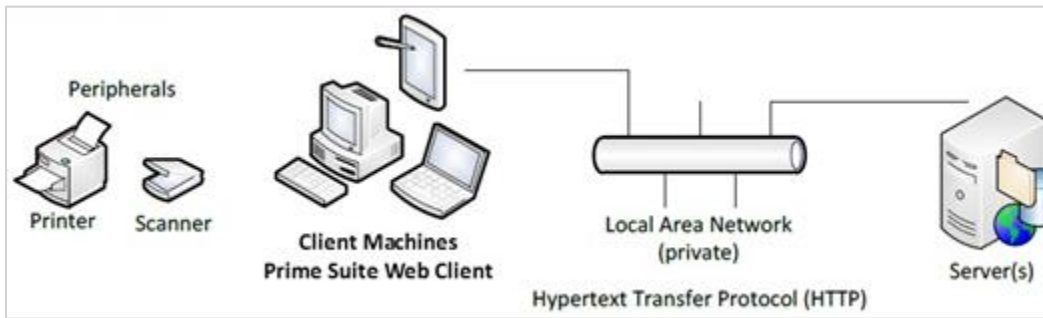
When deploying virtual machines (VM) guest systems in an environment that supports virtualization, each guest system is understood to be a separate server. An environment that deploys a web server and the database server to separate guest VM systems is described as a distributed deployment, even if both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

Refer to the [Deployment Options](#) section on page 16 for more information on the deployment of VMs in a Prime Suite environment.

Client Deployment

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

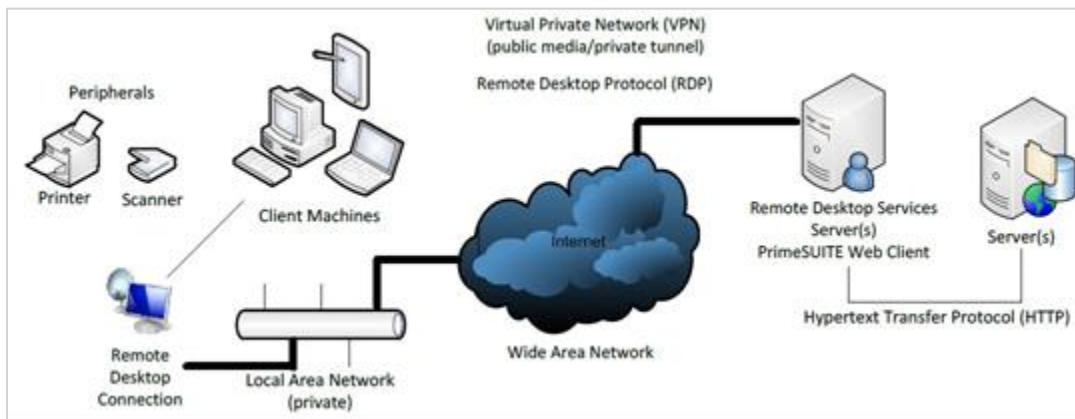
- Thick Client - This is the standard Prime Suite client, using a web browser and other program components installed on the local computer workstation. Communication with the server or servers always occurs on the same Local Area Network (LAN). This type of client may also be called the Browser Client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



The Thick Client requires a network connection speed of 300 Kbps per Prime Suite 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 Prime Suite program components installed when using the thin client. Instead, a remote connection program is used to connect to a remote desktop where the Prime Suite 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 Prime Suite 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 on page 34 for additional information about the supported versions of Microsoft Windows Server and associated Remote Desktop components.

Prime Suite+S Hosted Application

Instead of deploying servers in a Greenway customer computing environment, or in a datacenter managed by the customer, Prime Suite may instead be accessed in a hosted environment managed by Greenway. A simplified thin client architecture is used to connect to multi-tenant server systems managed by Greenway in partnership with Dell Services.

Prime Suite+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 Prime Suite 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 Prime Suite S+ clients.
- Microsoft Windows 10 Pro and Windows 10 Enterprise.

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 Prime Suite users. This VPN hardware is sold by Greenway for use with Prime Suite 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 Prime Suite users or located remotely. This VPN software is provided by Greenway for use with Prime Suite 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 Prime Suite S+.

Medical Devices

- Midmark and Welch Allyn brand devices, Thin Client compatible.

Printing

- Industry standard brand Microsoft Windows/XML Paper Specification (XPS) compatible devices.

Scanning

- Prime Suite only supports TWAIN scanners in the on-premise configuration. For hosted, or remote scanning, Greenway supports Citrix Scanner Redirection.
 - **Identification/Insurance Card:** We recommend the **Ambir ImageScan Pro 490i Duplex Scanner** that attaches directly to the station and uses a TWAIN driver.
 - **Document Scanning:** We recommend the **Fujitsu fi-7160 scanner** that attaches directly to the workstation and uses a TWAIN driver.

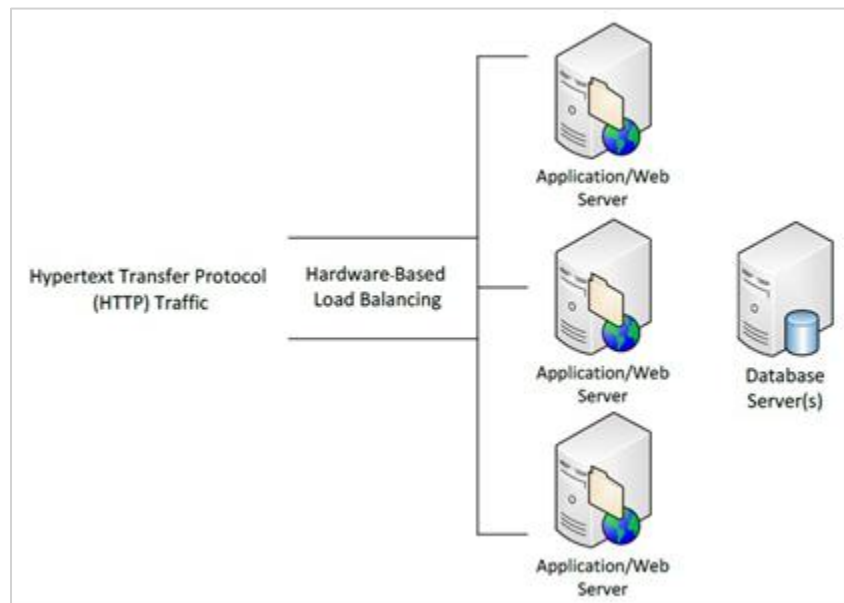
Deployment Options

To facilitate high availability and maximize the usage of computing resources, Prime Suite 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 Prime Suite, 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.

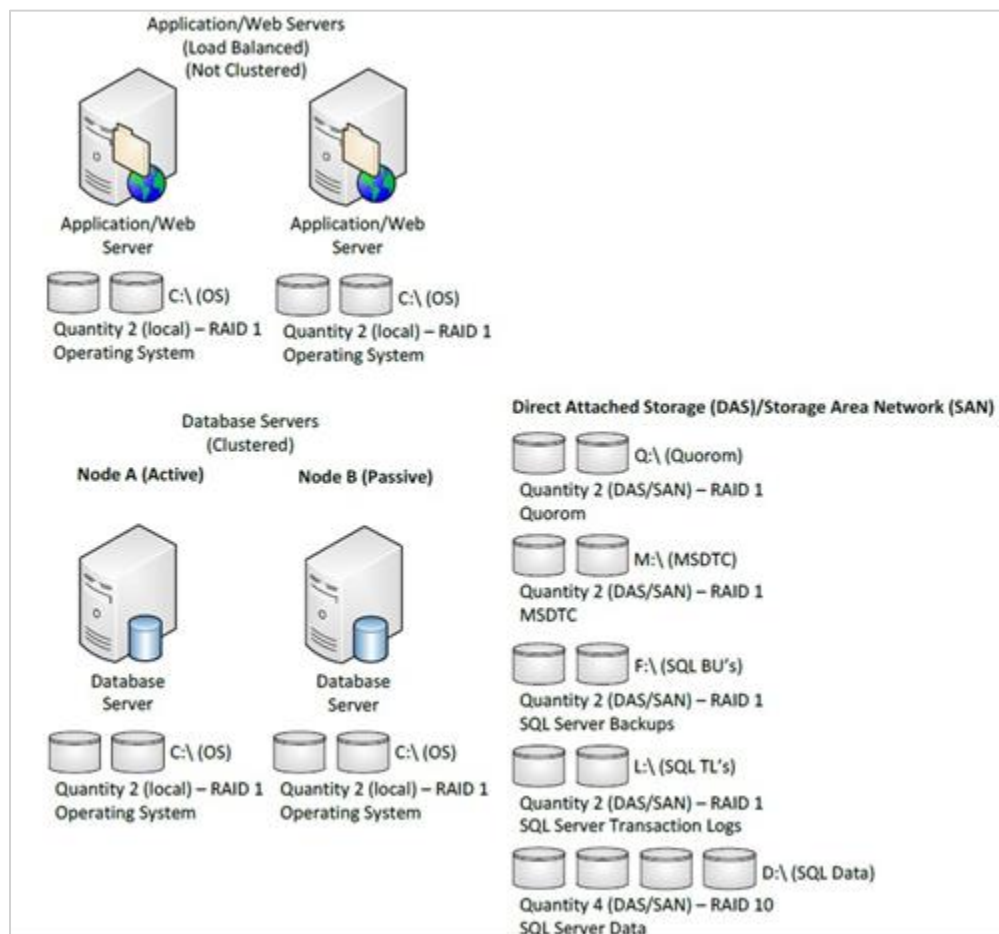
Clustering

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:

<http://msdn.microsoft.com/en-us/library/ms179410%28v=sql.105%29.aspx>

Clustering is possible with Prime Suite. However, the cluster is not supported by Greenway. Greenway only provides the information about the cluster requirements to get Prime Suite to work on it, and the cluster is supported by your local IT staff. The local IT staff must setup and configure the cluster before the new Prime Suite servers are built at Greenway. Our system requires only the Prime Suite side to see a single SQL server in a cluster whether through an AG Listener or a clustered MSDTC configuration.

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

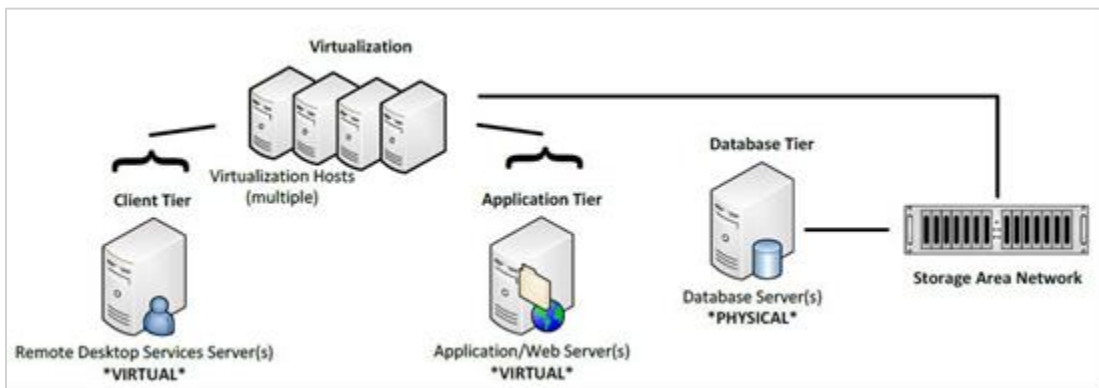


Virtualization

Specifications and requirements listed for Prime Suite 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 Prime Suite 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 34 for a comprehensive list of specifications.
- At a minimum, virtual application and web servers must be configured to use six 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 six 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 configured incorrectly, technicians and support personnel may observe high processor usage from the sqlservr.exe application process.

Note - For sites running VMWare VMs for the database server:

- Due to changes in VMWare vSphere 6.0 and above, Hyperthreaded Core Sharing can no longer be disabled; there will be a noticeable performance difference between a VMWare SQL Server and a non-VMWare SQL server. This performance loss is only seen on VMWare hosted SQL servers.
- Dynamic memory allocation should implement static memory.
- Memory Oversubscription/Overcommitment should not exceed the memory of the host.
- Do not make server images during the day.

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

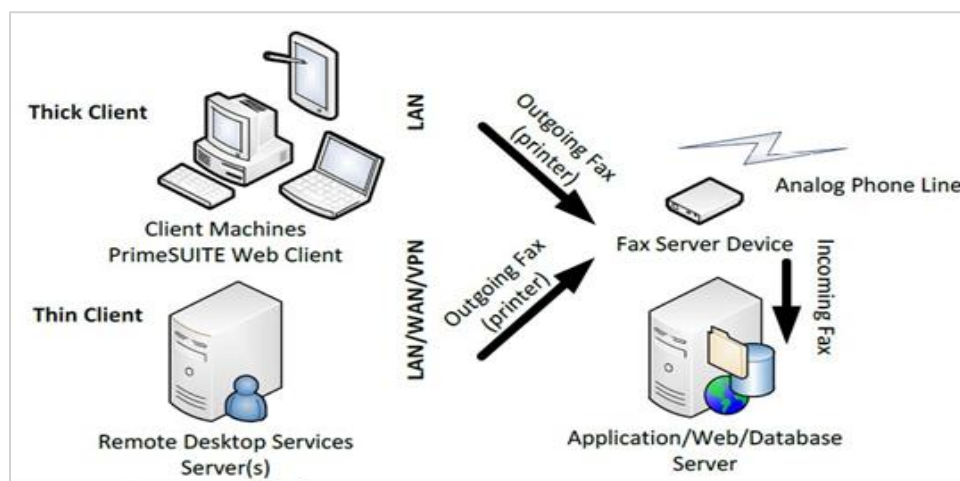
Prime Suite is engineered to connect to many leading diagnostic and vitals data devices. Stationary electrocardiography or mobile Holter, spirometry, stress, and vitals information may be entered into the Prime Suite database using a compatible device. Contact a Greenway sales representative for specific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

Fax Devices

Prime Suite 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, Updcox, or Providerflow.

It is recommended to use Updcox, or ProviderFlow to send fax as Greenway no longer sells the EHRfax MultiTech FaxFinder device.

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

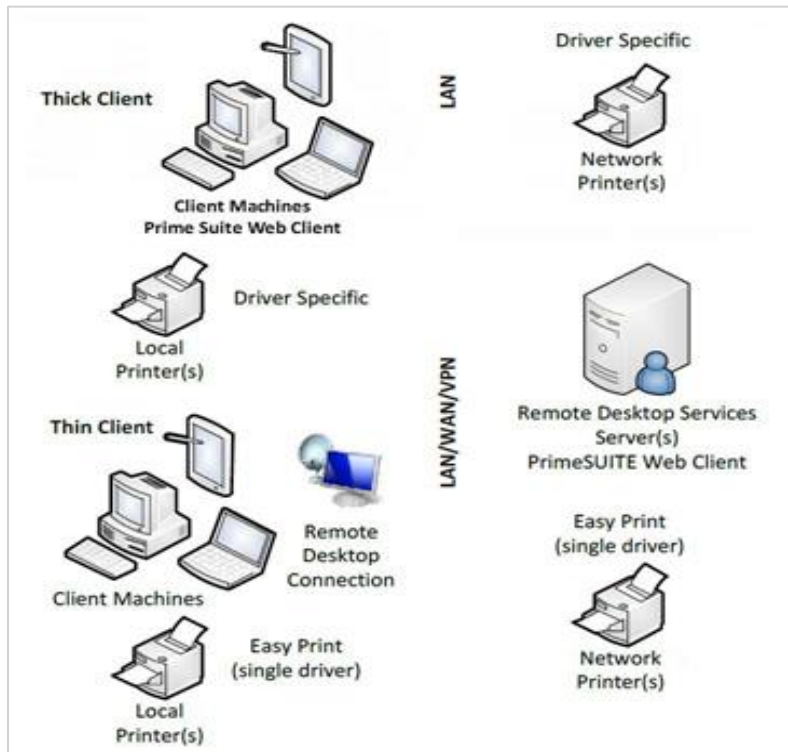


Printers

Prime Suite is coded to use standard printer calls and functions already present in Microsoft Windows. These functions include printers that are locally installed via an IP address 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:

<http://technet.microsoft.com/en-us/library/ff519199%28v=ws.10%29.aspx>

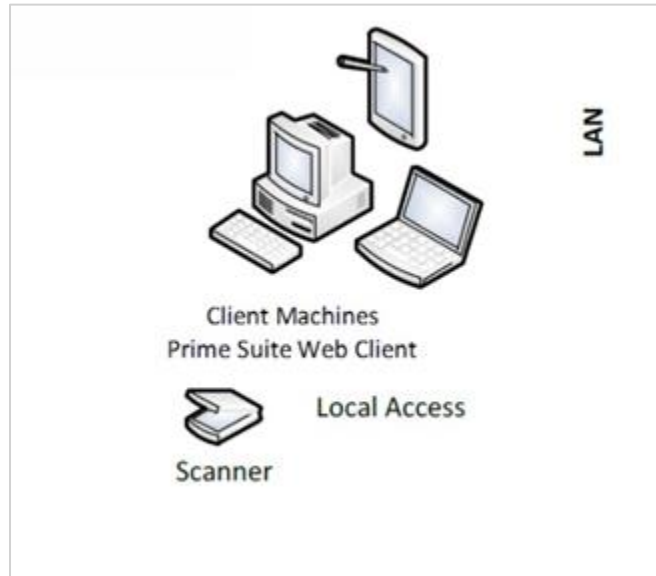
The following illustration depicts one example of a distributed printer configuration at a Prime Suite customer site, which includes locally installed printers.



Scanners

Prime Suite only supports TWAIN scanners in the on-premise configuration. For hosted, or remote scanning, Greenway supports Citrix Scanner Redirection.

The following illustrate depicts two examples of successful scanner device implementation in a Prime Suite environment.



Supporting Solutions

Greenway provides many additional services and software programs designed to enhance and expand the functionality of Prime Suite. 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

Prime Suite includes clinically-driven revenue cycle management (RCM) capabilities using Greenway Revenue Services. A team of billing experts drives a cloud-based software-as-a-service (SaaS) platform to provide RCM functionality without additional technical infrastructure. Greenway Revenue Services may be used for both on-premise and hosted Prime Suite +S customers.

For additional information regarding Greenway Revenue Services, refer to the following URL:

<http://www.greenwayhealth.com/solution/medical-billing-revenue-cycle-solutions/>

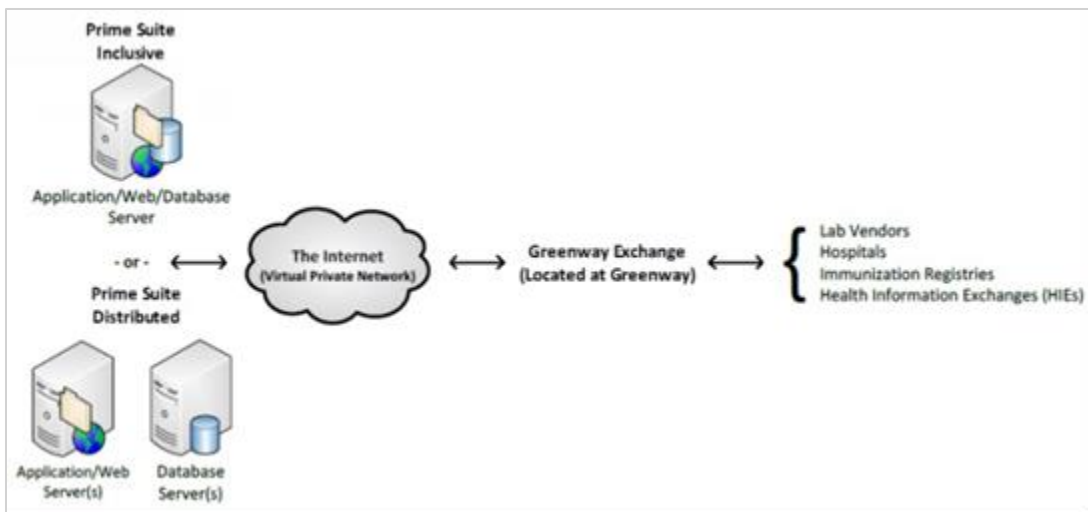
Application Programming Interface

The core Prime Suite 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://www.greenwayhealth.com/marketplace/>

Interoperability

Prime Suite enables data exchange through the Greenway Exchange 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.

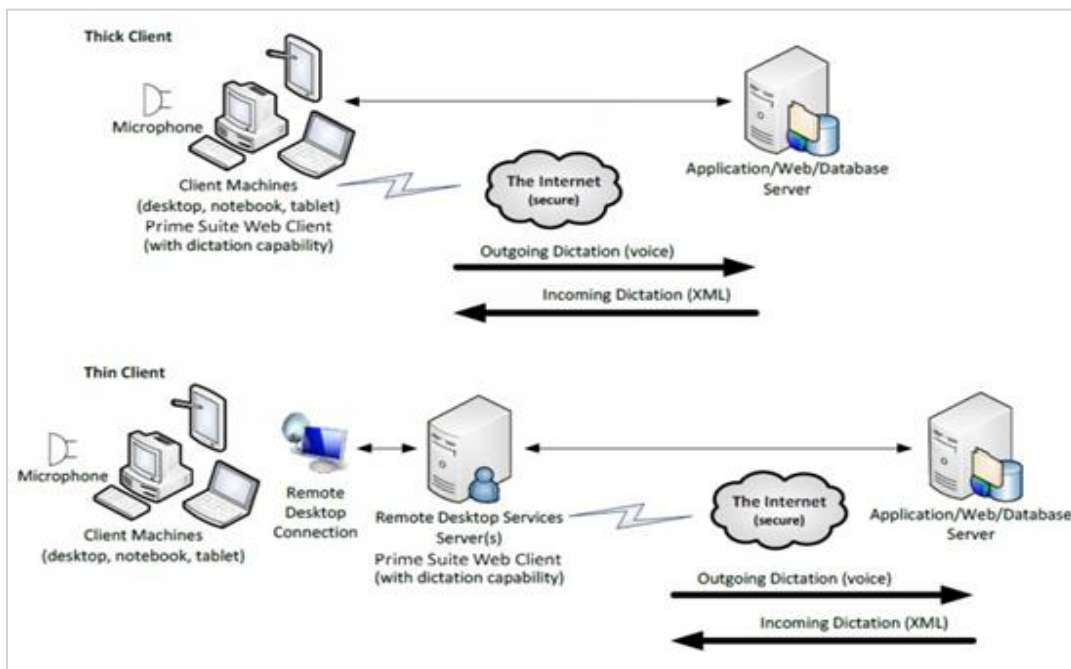


For detailed information regarding the Greenway Exchange service refer to the following URL:

<http://www.greenwayhealth.com/solution/clinical-connectivity/>

Dictation

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



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

For additional information regarding the Prime Speech solution, contact the Greenway Sales department, or contact us at <http://www.greenwayhealth.com/about-us/contact-us/>.

Data Cloud

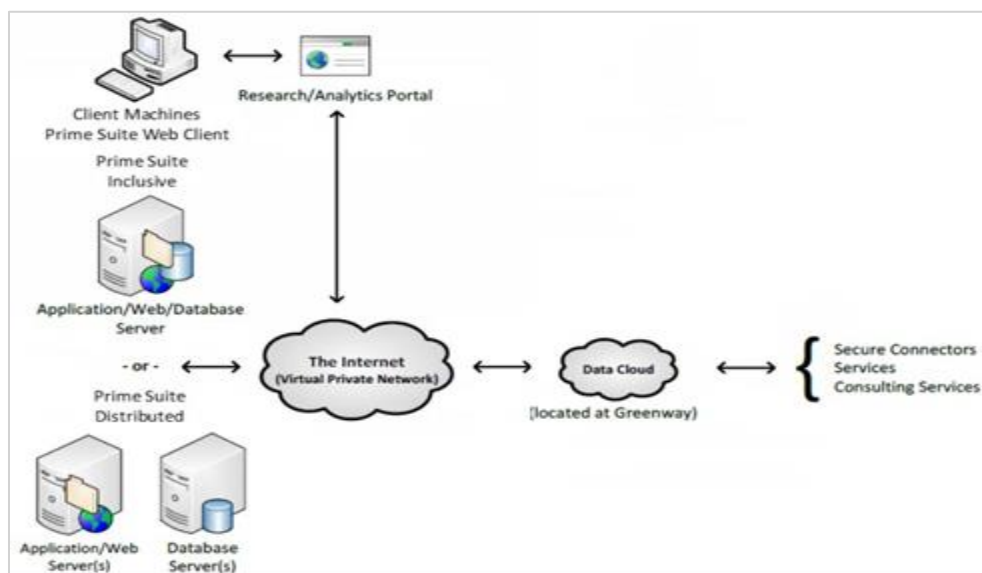
A number of Prime Suite features related to research and analysis are housed in Greenway Analytics, an Internet-hosted repository of capabilities intended to expand and to enhance the functionality of any Prime Suite implementation. A number of secure connectors and services are available.

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

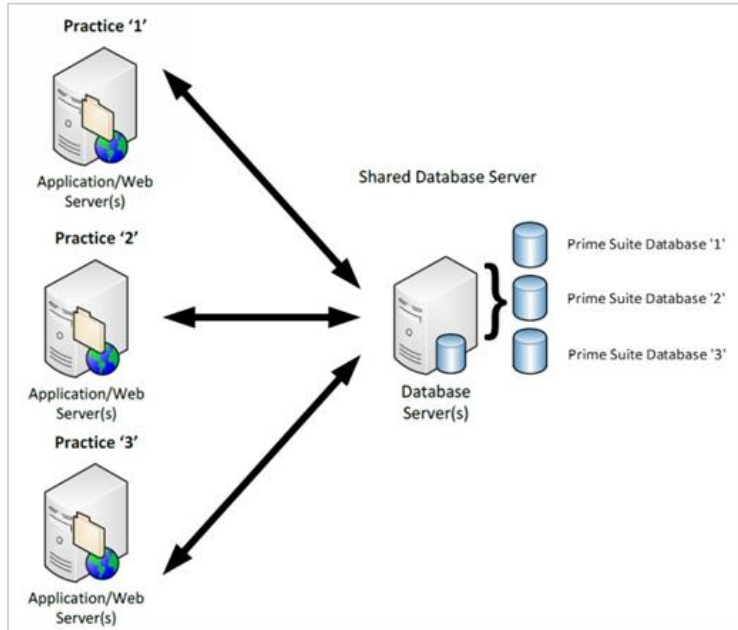
- Accountable Care Organization (ACO) services
- Clinical Decision Support (CDS) alerts
- Business Intelligence (BI) analysis and management
- Center for Medicare & Medicaid Services (CMS) Physician Quality Reporting System (PQRS) incentive
- CMS ePrescribe (eRx) incentive
- Community Document viewing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



Multi-tenant

Prime Suite 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 Prime Suite may be installed concurrently on a database server implemented for a multi-tenant environment.



Installation Environment Requirements

Any implementation of Prime Suite 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

A Prime Suite application server should not be used to provide any other networked services. It should not be a domain controller, mail server, etc. The Prime Suite server should not be used to run the Prime Suite client or act as a terminal server for any other interactive purpose. Using the server for purpose other than providing Prime Suite services can have unpredictable effects on the applications usability.

Access to the Prime Suite application should only be via a secure local network or remotely via an encrypted VPN tunnel. The server should not be available directly from the internet by direct addressing or port forwarding.

Servers implemented in a Prime Suite installation have general requirements that must be followed for a successful installation.

- **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.

Certain medical devices, such as imaging equipment, may cause wireless interference.

- **Internet for Remote Connectivity** - A full-time Internet connection is required for all Prime Suite 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.

- **Antivirus Software** – Do **not** install any antivirus software until after the Prime Suite installation process has been completed. Uninstall any existing software before beginning installation procedures.
- **User Account Control** – User Account Control (UAC) must be completely disabled before beginning any Prime Suite installation procedures.
- **Site Domain** – All Prime Suite servers must remain OFF a site's domain until after the Prime Suite installation process is completed.
- **8dot3** – 8dot3 must be enabled on local drives.
- **Server Dedication** – Servers must be dedicated to Prime Suite **only** and cannot be used by any other applications or databases.
- **SQL Media** – If SQL is not provided by Greenway Health, sites should provide a copy of the SQL media to Greenway Health. Greenway Health **must** install SQL on servers, regardless of who provided the SQL license to the site.

Desktop Environment Requirements

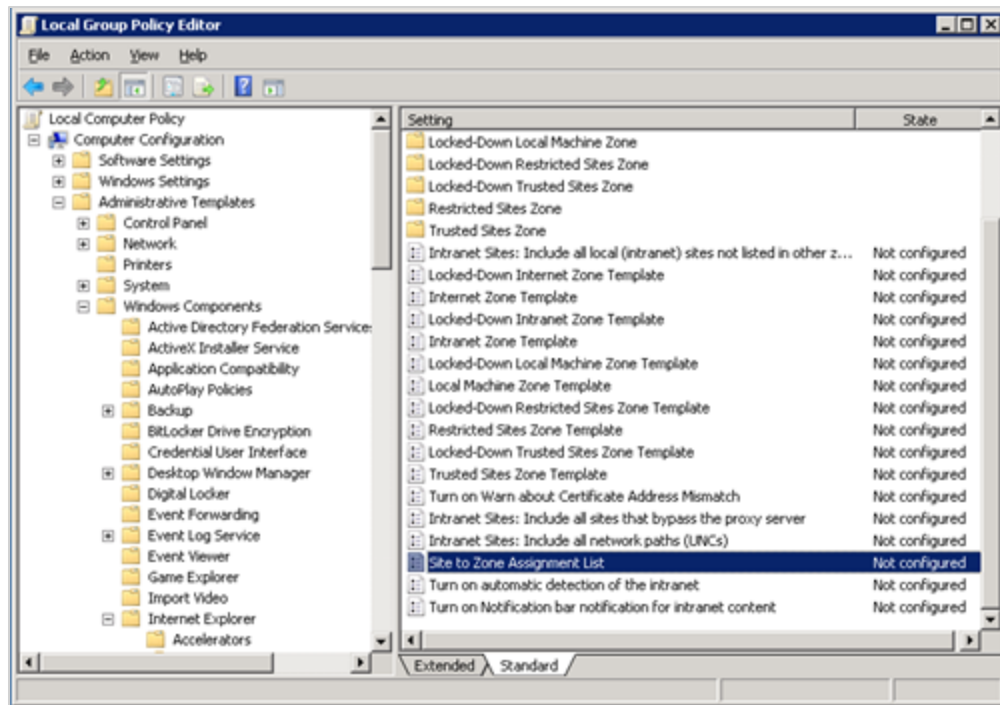
Microsoft Windows client workstations implemented in a Prime Suite environment require specific web browser settings for correct operation. When configuring the web browser, other settings related to web content filtering and Citrix client applications must also be configured. Use the information in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

Web Browser Settings

Prime Suite 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.

Note - *Internet Explorer 11 is now approved for installation on Prime Suite Servers v18.00.00.00 and up, including Application Servers, SQL Database servers, and Terminal Servers.*

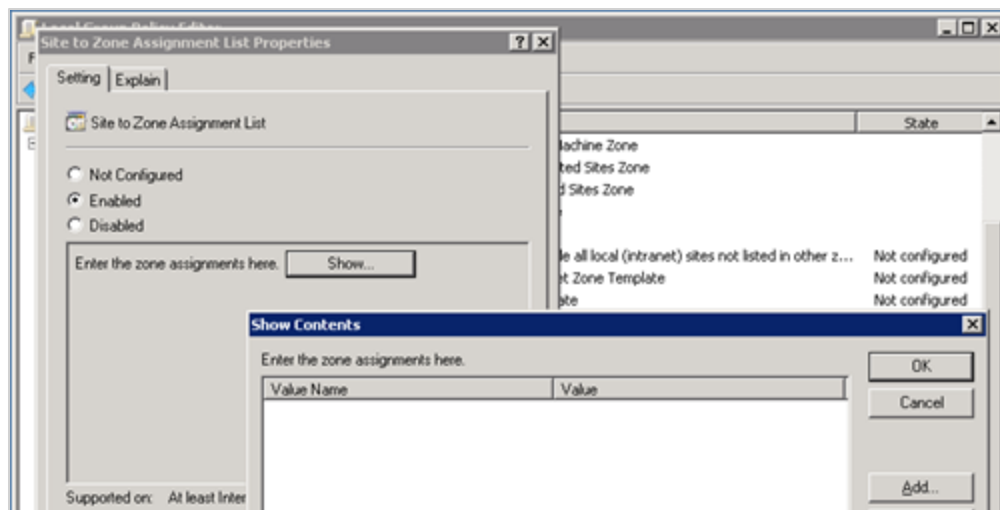
On the Microsoft Windows domain controller, or on the stand-alone Remote Desktop Services server, open the Local Group Policy Editor from the graphical user interface or with the command line instruction 'gpedit.msc'.



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:

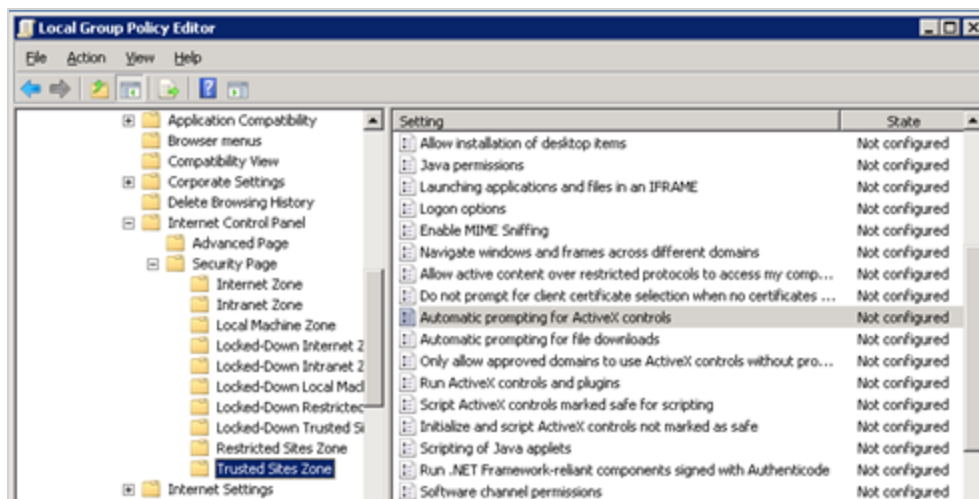
Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page

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 Prime Suite 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:

<http://technet.microsoft.com/en-us/library/cc725970.aspx>

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 Prime Suite and other Internet-based applications, HTTP web traffic used for Prime Suite 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

Prime Suite 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 Prime Suite client as a published application, to support Microsoft Windows user profile settings are 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 Prime Suite features and functions. All clients, servers, and network devices that are part of a Prime Suite installation must have open access to the following IP addresses and TCP ports.

Web Service Usage	Numeric IP Address	Protocol	Port
Claims, Electronic Remittance Advice (ERA) and Batch Eligibility	143.112.40.23	SFTP (Secure File Transfer)	22
	204.138.99.81	SFTP	22
	65.57.254.50	SFTP	22
	69.2.197.40	SFTP	22
	208.79.134.63	SFTP	22
Claims and ERA	205.216.7.14	SFTP	9922
	216.104.80.185	SFTP	22
Claims	74.63.172.37	SFTP	22
Statements	208.86.15.54	SFTP	22
	216.161.200.38	SFTP	22
	209.90.66.3	SFTP	22
Real-time Eligibility	143.112.40.27	SSL (Secure Sockets Layer)	443
	204.138.99.77	SSL	443
	64.57.254.44	SSL	7000
	69.2.197.41	SSL	443
Orders	170.138.220.93	SSL	443
ePrescribe	65.221.4.67	SSL	443
	65.221.4.102	SSL	443

Web Service Usage	Numeric IP Address	Protocol	Port
	65.221.4.103	SSL	443
	65.221.4.104	SSL	443
	65.221.4.107	SSL	443
	65.221.4.211	SSL	443
	65.221.4.216	SSL	443
	65.221.4.229	SSL	443
Dictation	66.45.73.253	SSL	443

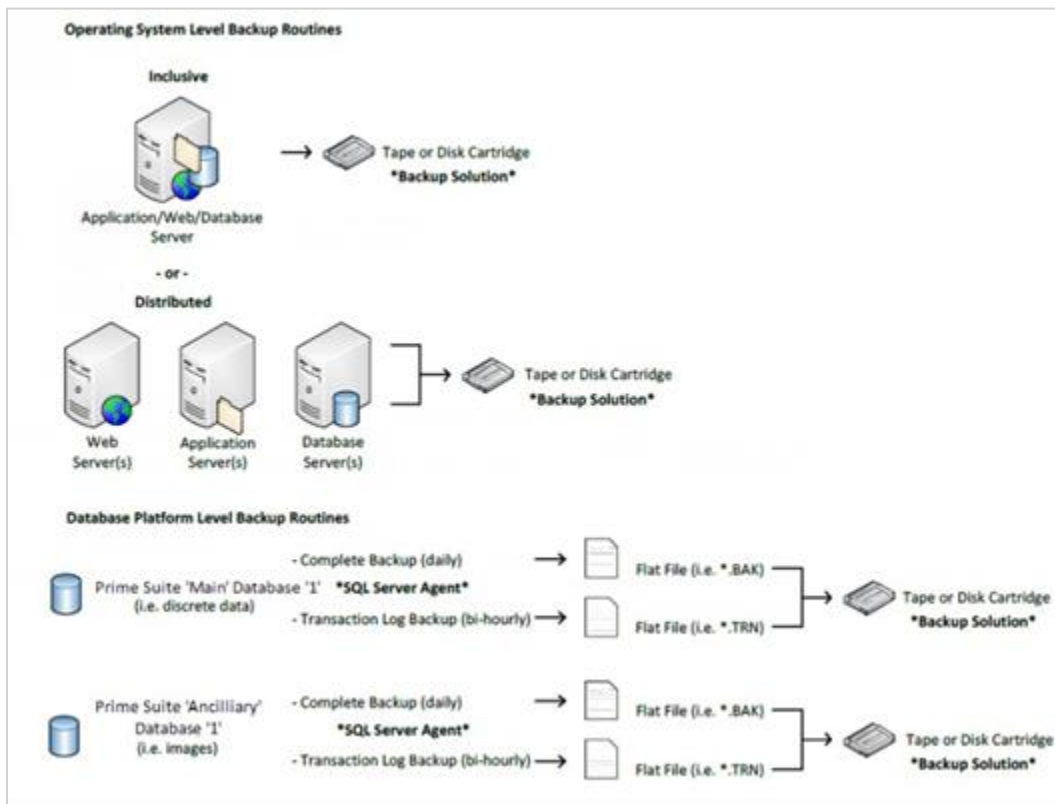
Installation Management

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

Back Ups

All Prime Suite 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 Prime Suite 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 Prime Suite system.

Malware Protection

All Prime Suite computing environments are required to include industry-standard virus and spyware protection software.

Remember - TrendMicro, WebRoot, Cylance, and BitDefender may be highly intrusive antivirus solutions and could harm the PrimeSuite installation. If any of these are used, take an image of the box after staging but before loading anti-virus software in case it irreparably damages the installation. A reload because of these utilities could cause additional charges.

Remember - Do not install malware or anti-virus software until your server(s) have been staged.

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

Also remember to include all local drives when taking an image of the servers before installing anti-virus software.

Additionally, the following are primary antivirus exclusions are also needed for Prime Suite to work properly. Some secondary settings may include network scanning and scripting scanning that may need to be disabled to allow Prime Suite to run properly.

- C:\Rcopia
- C:\InetPub
- C:\Greenway Medical Technologies\ADI
- C:\Program Files\Greenway Medical Technologies\Assemblies
- C:\Program Files\rmss
- C:\Greenway ADI
- C:\Prime Practice
- D:\Amyuni251
- D:\BioLink
- D:\FirstDataBank
- D:\Utilities
- D:\FaxArchive

- D:\Greenway ADI
- D:\peopleLYNK
- D:\PrimePractice
- D:\zfax
- D:\GMTBin
- D:\Program Files\MTS
- D:\SQLData or the SQL Database Instance Directories and Subdirectories.

Performance Monitoring

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

Monitoring Tool Type	Name
Built-in tools for clients and servers	Microsoft Windows Task Manager
Built-in tools for servers	Microsoft Windows Task Manager
	Microsoft Windows Performance Monitor
	Microsoft SQL Server Profiler
Downloadable tools	Microsoft Sysinternals http://technet.microsoft.com/en-us/sysinternals/default.aspx
	Process Monitor
	Process Explorer
	Fiddler Web Debugger http://www.fiddler2.com/fid

Security

Access to Protected Health Information (PHI) is restricted to authorized Prime Suite users via built-in application security. All access to PHI from outside the Prime Suite 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.

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

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

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

<http://msdn.microsoft.com/en-us/library/bb934049.aspx>

Hardware and Software Requirements

Prime Suite 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 Prime Suite system requirements, refer to the [Review Checklist](#) section on page 39 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 7.

Caution! - The following are guidelines for recommended configurations for Prime Suite setups. However, customers should consult with a Greenway engineer about their particular needs before actually configuring a server for use with Prime Suite.

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 11 for an explanation of inclusive and distributed server deployment models.

Inclusive Server Deployment Systems

User Sessions	Server Type	Minimum CPU	Minimum RAM	Disk and RAID requirement
1-10 users	Application/Web and Database	1 Intel Xeon, 6 cores	16 GB	(5) 300 GB 15K RPM (4) Disk RAID 10 with 1 Global Spare Note - It is recommended to use a SATA SSD, SAS SSD or SAS HDD
11-99 users	Application/Web and Database	1 Intel Xeon, 8 cores	32 GB	(5) 600 GB 15K RPM (4) Disk RAID 10 with 1 Global Spare Note - It is recommended to use a SATA SSD, SAS SSD or SAS HDD.

Distributed Server Deployment Systems

User Sessions	Server Type	Minimum CPU	Minimum RAM	Disk and RAID requirement
100 users per server	Application/Web	1 Intel Xeon, 8 cores	16 GB	(3) 300 GB 15K RPM (2) Disk RAID 1 with 1 Global Spare
100-250 users	Database	1 Intel Xeon, 8 cores	32 GB	(9) 600 GB 15K RPM (8) Disk RAID 10 with 1 Global Spare Note - It is recommended to use a SATA SSD, SAS SSD or SAS HDD
251-600 users	Database	2 Intel Xeon, 8 cores	48 GB	(9) 600 GB 15K RPM (2) Disk RAID 1 (6) Disk RAID 10 with 1 Global Spare Note - It is recommended to use a SAS SSD.
600-1,000 users	Database	2 Intel Xeon, 8 cores	48 GB	(11) 600 GB 15K RPM (2) Disk RAID 1 (2) Disk RAID 1 (6) Disk RAID 10 with 1 Global Spare Note - It is recommended to use a Flash SSD or SAS SSD.
1,001-2,500 users	Database	4 Intel Xeon, 8 cores	64 GB	(11) 600 GB 15K RPM (2) Disk RAID 1 (2) Disk RAID 1 (6) Disk RAID 10 with 1 Global Spare Note - It is recommended to use a Flash SSD or SAS SSD.

Other Server Deployment Systems

User Sessions	Server Type	Minimum CPU	Minimum RAM	Disk and RAID requirement
1-50 Remote Desktop	Remote Desktop Services client server	1 Intel Xeon, 8 cores	16 GB	(3) 300 GB 15K RPM (2) Disk RAID 1 with 1 Global Spare Note - It is recommended to use a SATA SSD, SAS SSD or

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).

Note - Greenway Health recommends the use of industry standard 6Gb/s SAS whenever possible.

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

Workstation hardware	Minimum CPU	Minimum RAM	Minimum Disk	Required network connection
Desktop	1 Intel Core 2 Duo Dual	4 GB	320 GB	1 Gigabit Ethernet
Notebook/Laptop	1 Intel Core i5 Dual Core	4 GB	320 GB	1 Gigabit Ethernet 1 Wireless 802.11 b/g/n
Tablet	1 Intel Core i5 Dual Core	4 GB	320 GB	1 Gigabit Ethernet 1 Wireless 802.11 b/g/n

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

Note - Greenway Health recommends the use of industry standard 6Gb/s SAS whenever possible.

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.

Setup Requirements

Prime Suite requires the operating system be loaded on the C: drive and application itself on a D: drive. This is typically accomplished by partitioning the recommended RAID 1 or RAID 10 (depending on the deployment method) container for Application/Web servers in a distributed environment into a 150GB C: drive and a 150GB D: drive.

In an inclusive environment where the database and web servers are on a single server, the drive lettering requirement is the same, and the sizing for the OS drive is the same, but the remainder of the RAID container should be partitioned as a D: drive for application and data.

For more information about additional setup requirements, see [Server and Networking Requirements](#).

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/WEBSERVER

- Microsoft Windows Server 2012 R2 Standard Edition, 64-bit only (HF20 only), or
- Microsoft Windows Server 2012 R2 Enterprise Edition, 64-bit only (HF20 only)

Note - *Internet Explorer 11 is now approved for installation on Prime Suite Servers v18.00.00.00 and up, including Application Servers, SQL Database servers, and Terminal Servers. Additionally, Windows Server 2012R2 Web Servers are only compatible with Prime Suite 18.00.00.20 or later.*

DATABASE SERVER

- Microsoft Windows Server 2012 R2 Standard Edition, 64-bit only (HF20 only), or
- Microsoft Windows Server 2012 R2 Enterprise Edition, 64-bit only (HF20 only)

- Microsoft SQL Server 2012 Standard Edition, or
- Microsoft SQL Server 2012 Enterprise Edition

Note - *You will need a separate server for your database server. It is required that the Microsoft SQL Server installation be done by Greenway personnel.*

REMOTE DESKTOP SERVICES SERVER

- Microsoft Windows Server 2012 R2 Standard Edition, 64-bit only (Terminal Services only)
- Microsoft Windows Server 2012 R2 Enterprise Edition, 64-bit only (Terminal Services only)

- Microsoft Windows Server 2016 R2 Standard Edition, 64-bit only (Terminal Services only)
- Microsoft Windows Server 2016 R2 Enterprise Edition, 64-bit only (Terminal Services only)

- Microsoft Internet Explorer 11 (*Compatibility Mode for 'greenwaymedical.com' must be enabled.)

- Adobe Acrobat Reader XI or later (required for use of Greenway Revenue Services supporting solution)

Clients

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

THICK CLIENT (BROWSER CLIENT)

- Microsoft Windows 10 Professional, 32-bit or 64-bit
- Microsoft Windows 10 Enterprise, 32-bit or 64-bit
- Microsoft Internet Explorer 11 (*Compatibility Mode for 'greenwaymedical.com' must be enabled.)
- Adobe Acrobat Reader XI or later (required for use of Greenway Revenue Services supporting solution)

THIN CLIENT (BROWSER CLIENT)

- Microsoft Windows 10 Professional, 32-bit or 64-bit, or
- Microsoft Windows 10 Enterprise, 32-bit or 64-bit, or
- Wyse ThinOS, or
- Linux

Portable Devices

Prime Mobile is the Prime Suite 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 Prime Mobile hardware requirements and prerequisites.

- Apple iOS: <https://appsto.re/us/te7H6.i>
- Google Android: <https://play.google.com/store/apps/details?id=com.greenway.primemobile>
- Microsoft Windows Phone/Mobile: <https://www.microsoft.com/en-us/store/p/prime-mobile/9wzdncrdt6l8>

Note - *Compatibility with Microsoft Windows Phone/Mobile is specific to the Prime Mobile application only. Refer to the previous section for client workstation requirements that apply to the standard thick client and thin client implementations of Prime Suite.*

Review Checklist

In many cases, review of the Prime Suite 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 Prime Suite 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 Prime Suite 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.

Check	Chec	Initial	Topic
<input checked="" type="checkbox"/>		_____	Application Architecture
<input checked="" type="checkbox"/>		_____	Application Security
<input checked="" type="checkbox"/>		_____	Deployment Models
	<input checked="" type="checkbox"/>		Server Deployment
	<input checked="" type="checkbox"/>		Client Deployment
<input checked="" type="checkbox"/>		_____	Prime Suite+S Hosted Application
<input checked="" type="checkbox"/>		_____	Deployment Options
	<input checked="" type="checkbox"/>		Load Balancing
	<input checked="" type="checkbox"/>		Clustering
	<input checked="" type="checkbox"/>		Virtualization
	<input checked="" type="checkbox"/>		Medical Devices
	<input checked="" type="checkbox"/>		Fax Devices
	<input checked="" type="checkbox"/>		Printers
	<input checked="" type="checkbox"/>		Scanners

Check	Check	Initial	Topic
<input checked="" type="checkbox"/>		_____	Supporting Solutions
	<input checked="" type="checkbox"/>		Clinically-driven Revenue Cycle Management
	<input checked="" type="checkbox"/>		Application Programming Interface
	<input checked="" type="checkbox"/>		Interoperability
	<input checked="" type="checkbox"/>		Enterprise Tasks
	<input checked="" type="checkbox"/>		Dictation
	<input checked="" type="checkbox"/>		Data Cloud
	<input checked="" type="checkbox"/>		Multi-tenant
<input checked="" type="checkbox"/>		_____	Installation Environment Requirements
	<input checked="" type="checkbox"/>		Server and Networking Environment Requirements
	<input checked="" type="checkbox"/>		Cooling
	<input checked="" type="checkbox"/>		Power
	<input checked="" type="checkbox"/>		Security
	<input checked="" type="checkbox"/>		Wired and Wireless Networking
	<input checked="" type="checkbox"/>		Internet for Remote Connectivity
	<input checked="" type="checkbox"/>		Desktop Environment Requirements
	<input checked="" type="checkbox"/>		Internet Service Requirements
<input checked="" type="checkbox"/>		_____	Installation Management
	<input checked="" type="checkbox"/>		Backups
	<input checked="" type="checkbox"/>		Microsoft Update
	<input checked="" type="checkbox"/>		Malware Protection
	<input checked="" type="checkbox"/>		Performance Monitoring
	<input checked="" type="checkbox"/>		Security
<input checked="" type="checkbox"/>		_____	Hardware and Software Requirements
	<input checked="" type="checkbox"/>		Client and Server Hardware
	<input checked="" type="checkbox"/>		Client and Server Software

_____	Greenway
BY (company name):	BY (company name):
_____	_____
(Authorized Signature)	(Authorized Signature)
_____	_____
(Typed or Printed Name)	(Typed or Printed Name)
_____	_____
(Title)	(Title)
_____	_____
(Date)	(Date)