SapphireIMS 5.0 Prerequisites v1.5.2

Restricted Rights Legend

This documentation is subject to and made available only pursuant to the terms of the Tecknodreams License Agreement and may be used or copied only in accordance with the terms of that agreement. It is against the law to copy the documentation except as specifically allowed in the agreement. This document may not, in whole or in part, be copied photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from Tecknodreams.

Information in this document is subject to change without notice and does not represent a commitment on the part of Tecknodreams.

Contents

1 Introduction

This document details the pre-requisites for installing and using SapphireIMS 5.0. These pre-requisites cover the areas of the hardware and software infrastructure required, the environment including port settings, security etc.

These pre-requisites are applicable for all editions of SapphireIMS and for all solutions. There are a few additional requirements for the Enterprise Plus edition and those are specifically marked.

This version applies to SapphireIMS 5.0 Patch Level 5004 or higher.

2 Server Hardware and Software Requirements

2.1 Hardware for SapphireIMS Server

The hardware infrastructure required to run SapphireIMS server is dependent on the edition, deployment architecture etc. and could vary. At the minimum, the hardware specifications for the SapphireIMS Server are as follows

- Intel Xeon Quad-Core Processor
- 16 GB RAM
- 300 GB Hard Disk
- Windows Server 2012 R2 /2016 / 2019 64 Bit

There will be 2 servers needed with the above specifications:

- User Acceptance Test (UAT) Server for configuration and acceptance testing. While not mandatory, this is required as a best practice especially if implementation is done in a phased manner and for ongoing support.
- Production Server.

In addition, depending on the solution and modules deployed, additional servers may be required to function as a Database server, Reporting Server, Web front end servers, data collectors etc. So also, implementation of High Availability and Disaster Recovery (DR) will require redundancy in hardware. In case you are using Enterprise or Enterprise Plus editions in a cluster or with probes, additional servers will be needed.

The Professional Services team will provide the exact hardware requirements after doing the sizing.

2.2 Operating Systems

SapphireIMS runs on Windows servers. The following versions of Windows Servers are supported

- Windows Server 2012 R2 (All editions)
- Windows Server 2016 (All editions)
- Windows Server 2019 (All editions)

2.3 Browsers Supported

SapphireIMS Web Portal is supported on the following browsers and best viewed with 1366x768 screen resolution:

Internet Explorer 10 and above
Google Chrome
Mozilla Firefox Version 11 and upwards

2.4 System Requirements for Optional Features

The following are system requirements for specific features if they are used.

2.4.1 Master Agent System Requirements

The Master Agent is a central agent (downstream server) on the same local network as other agents and which can centrally download and store patch files, scripts, and software. Using a Master Agent would reduce the network load since each agent system would not need to download the files individually from the Internet. The requirement for a dedicated Master Agent system is as below:

- Intel i3/i5/i7 Xeon Processor
- 8GB RAM
- 500GB Hard Disk
- Microsoft Windows 7 and above or Windows Server 2008 and above

OR

- Linux flavors like Ubuntu, Fedora, RedHat, Suse, Debian and OpenSuse

2.4.2 Cloud Connector System Requirements

The Cloud Connector is an optional component used when SapphireIMS server is running on the public cloud and the user information should be obtained from an Active Directory or LDAP server which is on-premise and for user authentication against active directory. The system requirements to run the Cloud Connector is as below:

- Intel i3/i5/i7 Xeon Processor
- 8GB RAM
- 100GB Hard Disk
- Microsoft Windows 7 and above or Windows Server 2008 and above

3 SapphireIMS SaaS

If SapphireIMS is running on SaaS, most of the pre-requisites pertaining to elements running on the customer network are applicable. In addition, the following is also a pre-requisite.

Web Portal URL	• There is a choice of configuring the SapphireIMS portal URL with 'sapphireims.com' domain or the customer domain. • For customer domain URL, the Customer needs to provide the URL Name, the SSL Certificate in the PFX File format and the Password for the same.

4 Port Details

SapphireIMS Server consists of the Engine, the MySQL Database and Web Portal component which support the various features provided by SapphireIMS application.

This section provides details on the ports which need to be opened along with the description, and the direction, along with where all it must be opened which could be the SapphireIMS Server and the Managed Systems. The ports need to be opened on any Network Firewalls as well if any systems are across the firewall.

The port requirements vary depending on whether an agent based, or agentless approach is used for data collection. In the case of agentless approach, the ports would depend on the protocol used.

While this section details the ports required for basic usage of SapphireIMS including user information import from Active Directory/ LDAP Server, Service Desk, discovering and collecting inventory information from systems, performing automation tasks like patch management and monitoring the performance of systems and network elements, there are additional requirements for ports to use specific features like application monitoring etc. and these are detailed in the individual sections.

Apart from these ports which apply to all editions, there are specific port requirements in the Enterprise and Enterprise Plus editions which are specified separately in this section.

4.1 Ports to be opened on the SapphireIMS Server

4.1.1 Ports for IT Asset Management and IT Service Management

Port	**Protocol**	**Purpose/Description**	**Source**	**Direction**	**Destination**
N/A	ICMP - Echo Request	Ping	SapphireIMS Server	Inbound/ Outbound	End Systems
3306	TCP	Communicating to the MySQL Server	SapphireIMS Server	Inbound	SapphireIMS Server if MySQL installed on the same server
80/443	TCP (HTTP/ HTPPS)	Web Portal Access	End User Systems	Inbound	SapphireIMS Server
5000 – 5030	UDP	SapphireIMS Internal communication	SapphireIMS Server	Local	SapphireIMS Server
5671/ 5672	TCP	SapphireIMS Internal communication	SapphireIMS Server	Local	SapphireIMS Server
80/443	TCP (HTTP/ HTPPS)	SapphireIMS Agent Communication	SapphireIMS Agent	Inbound	SapphireIMS Server
5671	TCP	Communicating with AD over the Internet using a Jump Server	SapphireIMS Jump Server	Inbound	SapphireIMS Server
162	UDP	For receiving SNMP Traps from SNMP End Nodes if monitoring is enabled	SapphireIMS Server	Inbound	SNMP End Points

4.1.2 Ports to be opened for Performance Monitoring

Port	Protocol	Purpose/Description	Source	Direction	Destination
514	UDP	Syslog data collection	End Nodes	Outbound	SapphireIMS Server
162	UDP	For receiving SNMP Traps and **used for Monitoring**	SNMP End Nodes	Outbound	SapphireIMS Server
9995	TCP	NetFlow data collection	End Nodes	Outbound	SapphireIMS Server
6343	TCP/UDP	sFlow data collection	End Nodes	Outbound	SapphireIMS Server
9200-9300	TCP	Used for storing collected logs in Elasticsearch	SapphireIMS	Local	SapphireIMS Server
9300-9400	TCP	Used for node to node communications	SapphireIMS	Local	SapphireIMS Server

4.2 Ports to be opened on the Managed Systems (for Agentless End Nodes)

The following ports need to be enabled in the Managed Systems which are Agentless. These include Windows systems, Linux or other Unix systems, Mac systems or network devices which are managed using SNMP protocol.

4.2.1 For Windows End Nodes using WMI *

Port	Protocol	Purpose/Description	Source	Direction	Destination
135	TCP	For remote management	SapphireIMS Server	Inbound	End Nodes
445	TCP	For network file sharing	SapphireIMS Server	Inbound	End Nodes
137	TCP	For accessing registry information	SapphireIMS Server	Inbound	End Nodes
49152 – 65535 (**)	TCP	Ports dynamically assigned in this range for use by WMI for remote data collection	SapphireIMS Server	Inbound	End Nodes

* Note – These WMI ports are also used for collecting Event Logs and Patch Management on Windows and for data collection from Hyper V servers.

** Note – To use a fixed port refer to the instructions given in the following link https://docs.microsoft.com/en-in/windows/win32/wmisdk/setting-up-a-fixed-port-for-wmi?redirectedfrom=MSDN. The settings must be done in each remote system.

4.2.2 For end nodes using SSH (Linux, Mac and other Unix systems)

Port	Protocol	Purpose/Description	Source	Direction	Destination
22	TCP	For SSH communication	SapphireIMS Server	Outbound	SSH nodes

4.2.3 For end nodes with SNMP enabled (Network Devices)

Port	Protocol	Purpose/Description	Source	Direction	Destination
161	UDP	For SNMP communication	SapphireIMS Server	Outbound	SNMP End Nodes
162	UDP	For receiving SNMP Traps and **used for Monitoring**	SNMP End Nodes	Outbound	

4.2.4 For end nodes managed with WBEM

Port	Protocol	Purpose/Description	Source	Direction	Destination
5988	TCP	WBEM communication	SapphireIMS Server	Outbound	WBEM enabled End Nodes
5989	TCP(SSL)	WBEM communication	SapphireIMS Server	Outbound	WBEM enabled End Nodes
898	TCP(SSL)	WBEM for Solaris End Nodes	SapphireIMS Server	Outbound	WBEM enabled End Nodes

4.2.5 For Storage Devices using CLI

Port	Protocol	Purpose/Description	Source	Direction	Destination
80/443	TCP (HTTP/ HTPPS)	EMC Storage	SapphireIMS Server	Outbound	EMC Storage Device

4.2.6 For Virtual Machines (VM)

Port	Protocol	Purpose/Description	Source	Direction	Destination
80/443	TCP (HTTP/ HTPPS)	For data collection from ESXi and XEN servers	SapphireIMS Server	Outbound	ESXi / XEN servers
For data collection from Hyper V servers, the ports to be opened are the same as for data collection using WMI					

4.3 Ports to be opened on Windows Agent Systems

Port	Protocol	Purpose/Description	Source	Direction	Destination
5027	UDP	For signaling purposes	Agent End Nodes	Local	Agent End Nodes
5028	UDP	For performance signals	Agent End Nodes	Local	Agent End Nodes
15000	UDP	Tray Icon Signal Port	Agent End Nodes	Local	Agent End Nodes
46001++	TCP	Agents to Master Agent communication for File Downloads	Agent End Nodes	Outbound	Master Agent Node

++ - Port to be opened on Master Agent Node

4.4 Ports to be opened on Linux and Mac Agent Systems

Port	Protocol	Purpose/Description	Source	Direction	Destination
22	TCP	For SSH communication	SapphireIMS Server	Outbound	SSH nodes
80/443	TCP (HTTP/ HTTPS)	For agent to communicate with server	End nodes	Outbound	SapphireIMS Server
46001++	TCP	For Agents to communicate with Master Agent for File Downloads	Agent End Nodes	Outbound	Master Agent Node

++ - Port to be opened on Master Agent Node

4.5 Ports to be opened for the Active Directory / LDAP Server

Port	Protocol	Purpose/Description	Source	Direction	Destination
389	TCP	For communications with the AD or LDAP Server to import user information	SapphireIMS Server	Outbound	AD / LDAP Server
636	TCP	For communications with the AD or LDAP Server to import user information. **Used when SSL is enabled**	SapphireIMS Server	Outbound	AD / LDAP Server

4.6 Ports to be opened for E-mail communications

Port	Protocol	Purpose/Description	Source	Direction	Destination
25/587	TCP	Communication with the SMTP Server for sending e-mails	SapphireIMS Server	Outbound	SMTP Server
110/ 587/ 465	TCP	Communication with POP3 / POP3 TLS/ POP3 SSL for receiving e-mails	SapphireIMS Server	Outbound	E-mail server
143/ 143/ 193	TCP	Communication with IMAP / IMAP TLS/ IMAP SSL for receiving e-mails	SapphireIMS Server	Outbound	E-mail server

4.7 Ports to be opened for Remote Control

Port	Protocol	Purpose/Description	Source	Direction	Destination
5900	TCP	UltraVNC port for remote control of the End Node	System used for taking the remote control	Outbound	End Node with UltraVNC server installed
5901	TCP	UltraVNC port on the Repeater	System used for taking the remote control	Outbound	Repeater node
4899	TCP	RAdmin port for remote control of the End Node	System used for taking the remote control	Outbound	End Node with RAdmin server installed
443	TCP (HTTPS)	For using MeshCentral for remote control	End Nodes with MeshCentral Agents installed	Outbound	MeshCentral Server located on the same system as the SapphireIMS Server

4.8 Ports required for Enterprise Edition

4.8.1 Ports required on the Cluster Server

Port	Protocol	Purpose/Description	Source	Direction	Destination
5000-5030	UDP	For internal communication purposes	SapphireIMS Cluster Server	Local	SapphireIMS Cluster Server

4.8.2 Ports required on the Cluster Member

Port	Protocol	Purpose/Description	Source	Direction	Destination
5012	UDP	For internal communication purposes	SapphireIMS Cluster Member	Local	SapphireIMS Cluster Member
3306	TCP	Communicating to the MySQL Server	SapphireIMS Cluster Member	Outbound	MySQL Server

4.9 Ports required for Enterprise Plus Edition (MSP)

4.9.1 Ports required on the MSP Server

Port	Protocol	Purpose/Description	Source	Direction	Destination
80/443	TCP (HTTP/ HTTPS)	For data replication from probes to the MSP Server	MSP Probes	Outbound	MSP Server

5 Services and Other Pre-requisites

5.1 SapphireIMS Server

SapphireIMS Server consists of the Engine and the Web Portal component which support the various features provided by SapphireIMS application. The pre-requisites required for these components are described below. These include the Services which must be running as well as other settings.

Services	The following services should be running, and the services should be configured to start automatically after system restart. Both the Display Name and the Service Name (in brackets) are given. • SapphireIMS Service (SapphireIMS) • SapphireMySQL (SapphireMySQL) or MySQL [In environments where MySQL is running on a different system, ensure that the service is running on the remote server] • Remote Procedure Call Service (RpcSs) • Windows Management Instrumentation Service (Winmgmt) • WMI Performance Adapter Service (wmiApSrv) • Server (LanmanServer)
Locale	• The servers on which SapphireIMS is installed must be set to English locale.

Antivirus Exceptions	• Before installation of SapphireIMS package/patch/agent, disable any antivirus software which may be running. • An exception rule must be added in the antivirus software to exclude <Installed Drive>\SapphireIMS folder from antivirus scans.
System Administrator Credentials	• Login as administrator to install SapphireIMS as all access privileges are required for SapphireIMS installation.

5.2 SapphireIMS Database

This section describes the pre-requisites for installing MySQL on Windows. For using MySQL on Linux refer to the MySQL Linux Guide document.

SapphireIMS takes daily backups of SapphireIMS database schema to preserve the collected data and the backup is preserved for 3 days. This backup uses the underlying MySQL database utilities. MySQL uses a temporary directory during its operations. This section describes the pre-requisite for this feature to work properly. This pre-requisite is also applicable for installation of patches during upgrades, as the patch installation utility performs a database backup before installing the patch.

The antivirus software should be configured appropriately to allow writing into the temporary folder. The default temporary folder used by MySQL is C:\WINDOWS\Temp and the same has to be excluded in the antivirus scans. If a different location other than the default is used by MySQL as the temporary directory, this needs to be determined and excluded.

Software components	• .NET Framework version greater or equal to 4.0 • Visual C++ Redistributable for Visual Studio 2010(32bit and 64 bit) • Visual C++ Redistributable for Visual Studio 2015-2019 (32bit and 64 bit) • For Microsoft Windows 2012 R2 OS the following two KB articles should be installed before installing MySQL 8 • KB2919442 • KB2919335

5.3 Pre-Requisites for Agentless Windows Systems

SapphireIMS supports management of Windows systems using Windows Management Instrumentation (WMI) protocol. The management includes discovery/inventory of Windows systems, monitoring of Windows systems and other system management features on Windows systems without using an agent on the managed nodes. This section describes the pre-requisites for this feature.

Services	The following services should be running, and the services should be configured to start automatically after system restart. Both the Display Name and the Service Name (in brackets) are given. • COM+ Event System (EventSystem) • Remote Procedure Call Service (RpcSs) • Remote Procedure Call Locator (RpcLocator) (Required for versions prior to Windows 7) • Windows Management Instrumentation Service (Winmgmt) • Workstation Service (LanmanWorkstation) • WMI Performance Adapter Service (wmiApSrv) • Server Service (LanmanServer) **Note:** • A WBEM test can be performed to confirm WMI details
Credentials	User Account with Domain Administrator privilege [For Windows Domain environment] or User Account with Local Administrator privilege [For Windows Workgroup environment]
Access Control	The following access control settings are available by default and should be verified. The User Account used should have sufficient privilege to launch remote processes for system management. Ensure the following policies are configured properly in Control Panel > Administrative Tools > Security Settings > Local Policies > User Rights Assignment. • Replace process level token • Adjust memory quotas for the project • Impersonate a client after authentication

	Ensure DCOM is configured properly by going to the Control Panel > Administrative Tools > Component Services > Console Root > Component Services >Computers > My Computer and then right click on it. In ‘Default Properties’ tab, • Property ‘Enable Distributed COM on this computer’ is checked • Property ‘Default Authentication Level’ is set to ‘Connect’ • Property ‘Default Impersonation Level’ is set to ‘Identify’ In ‘Default Protocols’ tab, • ‘Connection-oriented TCP/IP’ is present under DCOM protocols Remote User Account Control (UAC) should be disabled in Windows Vista and later OS if you are monitoring a target in a workgroup. This is a requirement when monitoring a workgroup computer. Disabling remote user account control does not disable local user account control functionality.

5.4 Pre-Requisites for Windows Systems using Agents

Services	The following services should be running, and the services should be configured to start automatically after system restart. Both the Display Name and the Service Name (in brackets) are given. • COM+ Event System (Event System) • Remote Procedure Call (RPC) (RpcSs) • Remote Procedure Call (RPC) Locator (RpcLocator) (Required for versions of Windows prior to Windows 7) • Server (LanmanServer) • Windows Management Instrumentation (Winmgmt) • WMI Performance Adapter (wmiApSrv) • Workstation (LanmanWorkstation) • Server (LanmanServer)
Anti-Virus exceptions prior to agent installation	The following folders need to be added as exceptions for Anti-virus scanning: ○ C:\Windows\Temp ○ C:\Users\<%USER%>\AppData\Local\Temp (The exception should be made for the account that is used for the installation) If the SapphireIMS Agent is going to be Installed using Active Directory then the Folder in which the Agent Installer will be copied by the AD in the target systems needs to be added in the Antivirus Exception Rule.

	If the SapphireIMS Agent is going to be Installed using SapphireIMS Automation Task then the path "<OS Drive>\ims" in the Target Systems needs to be added in the Antivirus Exception Rule. The following processes need to be added as exceptions: ○ SapphireIMSAgent-5.0-Setup.exe ○ SIMS_AgentTrigger.exe ○ <Agent Installer Package Name>.exe (<Agent Installer Package Name> is the name of the Agent Installer Package provided while creating it from the SapphireIMS UI)
Anti-Virus exceptions after installing SapphireIMS Agent	The following folders need to be added as exceptions for Anti-virus scanning: ○ <Windows Drive>\Program Files (x86)\SapphireIMSAgent The following processes need to be added as exceptions: ○ AgentServiceTray.exe ○ SapphireBackupTray.exe ○ SapphireIMSAgent.exe ○ SapphireIMSAgentUpgrade.exe ○ SIMS_AgentDiag.exe ○ SIMS_CommonSensor.exe ○ SIMS_TaskAgent.exe ○ SIMS_XMPPAgent.exe ○ sqlite3.exe ○ uninstall.exe ○ winvnc.exe ○ vncviewer.exe ○ 7z.exe

5.5 Discovery, Monitoring and System Management using SNMP

SapphireIMS supports management of systems using Simple Network Management Protocol (SNMP). This includes **Windows systems, Linux systems, other flavors of Unix systems, network devices** and any other devices that support management through SNMP protocol. This section describes the pre-requisites for this feature.

Services	The following services should be running, and the services should be configured to start automatically after system restart. - SNMP Service / Agents [Service name will vary based on the SNMP agent software used] - SNMP Trap Service [Required only if monitoring using SNMP Traps is used. Service name will vary based on the SNMP software used]
Credentials	For SNMP V1 and V2, - SNMP read community string For SNMP V3, - Security Name - Security Authorization Protocol and Password - Security Privacy Protocol and Password
Notes	SNMP devices must have unique 'snmpEngineID' in the network for successful discovery and data collection.

5.6 Discovery, Monitoring and System Management for Agentless Systems using SSH

SapphireIMS supports management of systems using SSH protocol. This includes **Linux systems and other UNIX flavors like Solaris, AIX etc.** This section describes the pre-requisites for this feature.

Access Control	If a user account with 'sudo' privilege is used for discovery, the following permission should be configured to allow discovery scripts to run remotely without a terminal. If the line "Defaults requiretty" is present in /etc/sudoers file, it has to be **commented or removed**. Alternately, the line can be modified as "Defaults :<username> requiretty" to allow only a specific user to run scripts without terminal.

5.7 Pre-Requisites for Linux and Mac Agent based Systems

Miscellaneous	- Linux or Mac agents should be installed either from root or an account with sudo privileges - End system should have Python Version 2.6 or above installed - End system should have sqlite3 Python module installed

Linux	The following commands need 'sudo' access with NOPASSWD tag. /bin/mkdir, /bin/tar, /bin/mv, /bin/find, /bin/kill, /bin/cp, /bin/ls, /bin/chmod, /bin/chown, /bin/rm, /usr/sbin/dmidecode, /usr/sbin/rhn_check, /sbin/ethtool, /usr/sbin/smartctl, /dev/mem, /etc/init.d, /sbin/ifconfig, /usr/bin/test, /usr/bin/crontab, /usr/bin/unzip, /usr/bin/apt-get, /usr/bin/yum, /usr/bin/zypper, $$LINUX_AGENT_INSTALL_PATH$$/SapphireIMSAgent/scripts/lshw, netstat, cat, /sbin/route, /var/tmp /bin/zcat, /bin/gzcat, /proc/cpuinfo, /etc/sysconfig/rhn/systemid, /etc/*-release, /proc/meminfo, /etc/resolv.conf, df, ps, dpkg-query, rpm, /etc/sudoers, /etc/visudo, visudo, /etc/oraInst.loc, /var/opt/oracle/oraInst.loc, $$PYTHON_PATH$$, shutdown, dos2unix, /sys/block, /dev/disk/by-path, iostat, /dev/, /dev/null, pkill $$LINUX_AGENT_INSTALL_PATH$$ refers to the SapphireIMSAgent installation path $$PYTHON_PATH$$ refers to the path where Python is installed
MacOS	The following commands need 'sudo' access with NOPASSWD tag. /bin/mkdir, /bin/tar, /bin/mv, /bin/find, /bin/kill, /bin/cp, /bin/ls, /bin/chmod, /bin/chown, /sbin/chkconfig, /usr/sbin/update-rc.d, /bin/rm, /sbin/ifconfig, /usr/bin/crontab, /usr/bin/unzip, /Applications/, netstat, cat, system_profiler, /sbin/route, /var/tmp, /bin/zcat, /bin/gzcat, /etc/resolv.conf, df, ps, /etc/sudoers, fdesetup, /usr/sbin/sysctl, /bin/launchctl, /etc/visudo, visudo, $$PYTHON_PATH$$, shutdown, dos2unix, /dev/disk/by-path, /dev/, systemsetup, /dev/null, pkill $$LINUX_AGENT_INSTALL_PATH$$ refers to the SapphireIMSAgent installation path $$PYTHON_PATH$$ refers to the path where Python is installed

Notes	The SapphireIMS server should be reachable A Master Agent is required for patching (Ubuntu) and script deployment.
Linux Flavors supported	• Ubuntu • Fedora • Suse • OpenSuse • RedHat • Debian
MacOS Versions supported	• 10.10: "Yosemite" • 10.11: "El Capitan" • 10.12: "Sierra" • 10.13: "High Sierra" • 10.14: “Mojave • 10.15: “Catalina”

5.8 Pre-Requisites for AIX Systems

AIX	The following commands need ‘sudo’ access with NOPASSWD tag. /usr/bin/tar, /var/tmp, /usr/bin/ls, /usr/bin/rm, /usr/bin/mkdir, /usr/sbin/smtctl, /usr/bin/tar, /usr/bin/zcat, /usr/bin/gzcat, netstat, cat, df, iostat, /bin/ps, /usr/bin/crontab, /usr/sbin/lscfg, /usr/sbin/lsconf, /bin/lslpp, /usr/bin/svmon, /usr/sbin/ifconfig, /usr/bin/lparstat, /usr/bin/uptime, /usr/bin/vmstat, $$SAPP-SCRIPT-INSTALL-PATH$$ SAPP-SCRIPT-INSTALL-PATH refers to the path where agentless scripts will be installed (this is defined in the Global Settings in SapphireIMS. The setting name is 'SSH scripts install path', and the default value is '/opt/SapphireIMS')

5.9 Discovery, Monitoring and System Management using WBEM

SapphireIMS supports management of systems using Web Based Enterprise Management (WBEM) Protocol. This includes **Linux systems, Solaris, ESXi, storage devices** and any other devices that support management through WBEM protocol. This section describes the pre-requisites for this feature.

Services	The following services should be running, and the services should be configured to start automatically after system restart. • WBEM Service [Service name will vary based on the WBEM software used]
Credentials	• WBEM Username and Password • If SSL is enabled, a certificate is required.

6 Discovery, Monitoring and System Management of Virtual Machines

SapphireIMS supports management of systems using Virtual Machine (VM) application discovery. This includes **VMware, Hyper-V and Xen** virtual machine servers. This section describes the pre-requisites for this feature.

Services	The following services should be running, and the services should be configured to start automatically after system restart. • VIM Service for VMware server • Microsoft Hyper-V services for Hyper-V server
Credentials	• VM Username and Password

7 Monitoring MS Exchange Server 2010, 2013

Using SapphireIMS, you can monitor Microsoft Exchange. The pre-requisites on the SapphireIMS Server as well as the MS Exchange server are given below.

7.1 Pre-Requisites for SapphireIMS Server

Software components	• .NET Framework version greater or equal to 4.0 • PowerShell version greater or equal to 2

7.2 Pre-Requisites for the node running MS Exchange Server

Services	• Windows Management Instrumentation Service (Winmgmt)

8 Identity Providers

SapphireIMS integrates with Identity Providers which are based on SAML and OAuth 2 protocols, for authentication services.

8.1 Pre-Requisites for ADFS using SAML 2.0

Environment	• Fully configured AD and ADFS setup (refer to user manual for details) • Federation Metadata file generated in ADFS • HTTPS should be enabled in SapphireIMS.

8.2 Pre-Requisites for OAuth 2 (Google, Microsoft Office 365)

Google	• SapphireIMS should be enabled for SSL communication using https. • SapphireIMS should be registered with the service and the Client ID and Client Secret needs to be obtained. Refer to the User Manual for details. • Users logging in to Sapphire using OAuth2 should have Google accounts created. The users should be imported into SapphireIMS (using Excel user import). Note that the e-mail id for the users should be the Google mail id.
Office 365	• SapphireIMS should be enabled for SSL communication using https. • SapphireIMS application needs to be registered with Azure Portal. For the registered application, Client-ID and Client Secret should be obtained from Azure. Refer to the User Manuals for details.

	• Users in SapphireIMS should have an Office 365 account. The users should be imported into SapphireIMS (using Excel user import).

9 Cloud Connector

SapphireIMS Cloud Connector component is used to import user information from the on-premise Active Directory when SapphireIMS is hosted on the cloud. This section describes the pre-requisites for this feature.

Services	The following services should be running, and the services should be configured to start automatically after system restart. • SapphireIMSCloudConnector

10 Windows Patch Management

SapphireIMS supports scanning and deployment of Windows patches on Windows managed nodes. In an agent-less environment, the patches are downloaded into SapphireIMS Server and deployed to the Windows nodes. In an agent environment, optionally a master agent system can be setup for downloading the patches instead of all agent systems downloading patches. The pre-requisites on the Windows managed nodes vary based on the version of the operating system installed. This section describes the pre-requisites for this feature.

10.1 Pre-Requisites for Windows Patch Management

Services	The following services should be running, and the services should be configured to start automatically after system restart. • Background Intelligent Transfer Service (BITS) • Windows Update [Only in Windows 7 and Windows 2008] (wuauserv) • Windows Management Instrumentation Service (Winmgmt)
Notes	• An Internet connection for the SapphireIMS server is required for downloading Windows patches. In case of MSP edition, the Internet connection is required for the probe server also. The Microsoft sites given

	below must be white listed in the SapphireIMS server to download the patches. ○ http://go.microsoft.com/fwlink/?LinkID=74689 ○ http://update.microsoft.com/redist/wuredist.cab ○ http://www.download.windowsupdate.com/* ○ http://download.windowsupdate.com/* • If a proxy is enabled in the network, make sure the settings are properly configured in SapphireIMS. • Windows Update Redistribution URL is provided by default under SapphireIMS Windows patch management settings. Download this cab file to perform the 'Windows Update Agent' installation. If the target system version is less than the stated client version, then SapphireIMS will automatically install WUA at the time of performing a scan. This cab file has updates based on three processor platform types as given below • 'x86' (For 32-bit editions of Windows) • 'x64' (For 64-bit editions of Windows) • 'ia64' (For Itanium based)

10.2 Pre-Requisites for SapphireIMS Agent Nodes and Master Agent Nodes

Services	The following services should be running, and the services should be configured to start automatically after system restart. • BITS – Background Intelligent Transfer Service • Windows Update [Only in Windows 7 and Windows 2008]
Notes	• Ensure remote network share is allowed from SapphireIMS for Agent Less Nodes. • Ensure the Master agents are up and running. • Ensure sufficient disk space is available on SapphireIMS server and all the Master agents.

10.3 Pre-Requisites for Windows Online Patch Scan

SapphireIMS supports online patch scan for Windows machines. For this, the below pre-requisites must be enabled in the managed node.

Notes	• Internet connectivity must be available • “Receive updates for other Microsoft products when you update Windows” option must be enabled under windows update advanced settings. • An Internet connection for the SapphireIMS server is required for downloading Windows patches. In case of MSP edition, the Internet connection is required for the probe server also. The Microsoft sites given below must be white listed in the SapphireIMS server to download the patches. ○ http://windowsupdate.microsoft.com ○ http://*.windowsupdate.microsoft.com ○ https://*.windowsupdate.microsoft.com ○ http://*.update.microsoft.com ○ https://*.update.microsoft.com ○ http://*.windowsupdate.com ○ http://download.windowsupdate.com ○ http://download.microsoft.com ○ http://*.download.windowsupdate.com ○ http://ntservicepack.microsoft.com ○ http://wustat.windows.com

11 Linux Patch Management using Agents

SapphireIMS supports scanning and deployment of Linux patches on Linux managed nodes using Agents.

Notes	• For Fedora, Red Hat, SUSE, OpenSUSE and Centos patch management Internet access is required in the target system for scanning and deployment of patches • For Ubuntu Linux Agent patch management Internet access is required in the SapphireIMS Server for scanning and deployment of patches. The following URLs need to be white listed for access ○ http://archive.ubuntu.com/ubuntu/dists/precise/* ○ http://archive.ubuntu.com/ubuntu/dists/precise-updates/* ○ http://archive.ubuntu.com/ubuntu/dists/precise-security/*

	○ http://archive.ubuntu.com/ubuntu/dists/precise-proposed/* ○ http://archive.ubuntu.com/ubuntu/dists/precise-backports/* ○ http://security.ubuntu.com/ubuntu/dists/precise/* ○ http://security.ubuntu.com/ubuntu/dists/precise-updates/* ○ http://security.ubuntu.com/ubuntu/dists/precise-security/* ○ http://security.ubuntu.com/ubuntu/dists/precise-proposed/* ○ http://security.ubuntu.com/ubuntu/dists/precise-backports/* ○ http://archive.ubuntu.com/ubuntu/dists/trusty/* ○ http://archive.ubuntu.com/ubuntu/dists/trusty-updates/* ○ http://archive.ubuntu.com/ubuntu/dists/trusty-security/* ○ http://archive.ubuntu.com/ubuntu/dists/trusty-proposed/* ○ http://archive.ubuntu.com/ubuntu/dists/trusty-backports/* ○ http://security.ubuntu.com/ubuntu/dists/trusty/* ○ http://security.ubuntu.com/ubuntu/dists/trusty-updates/* ○ http://security.ubuntu.com/ubuntu/dists/trusty-security/* ○ http://security.ubuntu.com/ubuntu/dists/trusty-proposed/* ○ http://security.ubuntu.com/ubuntu/dists/trusty-backports/* ○ http://archive.ubuntu.com/ubuntu/dists/xenial/* ○ http://archive.ubuntu.com/ubuntu/dists/xenial-updates/* ○ http://archive.ubuntu.com/ubuntu/dists/xenial-security/* ○ http://archive.ubuntu.com/ubuntu/dists/xenial-proposed/* ○ http://archive.ubuntu.com/ubuntu/dists/xenial-backports/* ○ http://security.ubuntu.com/ubuntu/dists/xenial/* ○ http://security.ubuntu.com/ubuntu/dists/xenial-updates/* ○ http://security.ubuntu.com/ubuntu/dists/xenial-security/* ○ http://security.ubuntu.com/ubuntu/dists/xenial-proposed/* ○ http://security.ubuntu.com/ubuntu/dists/xenial-backports/* ○ http://archive.ubuntu.com/ubuntu/dists/bionic/* ○ http://archive.ubuntu.com/ubuntu/dists/bionic-updates/* ○ http://archive.ubuntu.com/ubuntu/dists/bionic-security/* ○ http://archive.ubuntu.com/ubuntu/dists/bionic-proposed/* ○ http://archive.ubuntu.com/ubuntu/dists/bionic-backports/* ○ http://security.ubuntu.com/ubuntu/dists/bionic/* ○ http://security.ubuntu.com/ubuntu/dists/bionic-updates/* ○ http://security.ubuntu.com/ubuntu/dists/bionic-security/* ○ http://security.ubuntu.com/ubuntu/dists/bionic-proposed/* ○ http://security.ubuntu.com/ubuntu/dists/bionic-backports/* ○ http://archive.ubuntu.com/ubuntu/dists/disco/* ○ http://archive.ubuntu.com/ubuntu/dists/disco-updates/* ○ http://archive.ubuntu.com/ubuntu/dists/disco-security/* ○ http://archive.ubuntu.com/ubuntu/dists/disco-proposed/* ○ http://archive.ubuntu.com/ubuntu/dists/disco-backports/* ○ http://security.ubuntu.com/ubuntu/dists/disco/* ○ http://security.ubuntu.com/ubuntu/dists/disco-updates/* ○ http://security.ubuntu.com/ubuntu/dists/disco-security/*

	○ http://security.ubuntu.com/ubuntu/dists/disco-proposed/* ○ http://security.ubuntu.com/ubuntu/dists/disco-backports/* ○ http://archive.ubuntu.com/ubuntu/dists/focal/* ○ http://archive.ubuntu.com/ubuntu/dists/focal-updates/* ○ http://archive.ubuntu.com/ubuntu/dists/focal-security/* ○ http://archive.ubuntu.com/ubuntu/dists/focal-proposed/* ○ http://archive.ubuntu.com/ubuntu/dists/focal-backports/* ○ http://security.ubuntu.com/ubuntu/dists/focal/* ○ http://security.ubuntu.com/ubuntu/dists/focal-updates/* ○ http://security.ubuntu.com/ubuntu/dists/focal-security/* ○ http://security.ubuntu.com/ubuntu/dists/focal-proposed/* ○ http://security.ubuntu.com/ubuntu/dists/focal-backports/* • The following Sudo access privileges are additionally required /var/lib/apt/lists/ /etc/apt/ /var/cache/apt/archives

12 Third Party Patch Management (TPPM)

SapphireIMS supports patch management for application software on Windows and MacOS. It can scan for missing application patches and then uses a 3rd party application repository (Chocolatey for Windows and Homebrew for MacOS) to obtain the package details which is then used to run the commands to upgrade in a silent mode.

12.1 Pre-Requisites for Windows TPPM

Notes	• The following URL needs to be white listed https://chocolatey.org/* • The download URL for the specific software should also be white listed. This URL can be obtained from the patch details screen after the patch scan is done.

12.2 Pre-Requisites for Mac TPPM

Notes	• The following URL needs to be white listed https://formulae.brew.sh/api/cask/

	• The download URL for the specific software should also be white listed. This URL can be obtained from the patch details screen after the patch scan is done. • The following Sudo access privileges are additionally required /Volumes/scripts/* /Applications/* /usr/bin/Hdiutil

13 SapphireIMS E-mail Communications

SapphireIMS allows sending notifications through emails. The notification feature sends emails using the SMTP protocol. The local SMTP server should be configured in SapphireIMS to enable notification feature. SapphireIMS can also receive e-mails from servers using POP3/IMAP protocols and this is used in email to Service Desk Records conversion feature. This section describes the pre-requisites for this feature.

Other Configurations	For Microsoft Exchange Server, • SMTP Connector should be installed and configured • SMTP should allow support for 'AUTH_COMMAND' For other mail servers • SMTP Server should be enabled and configured

14 Advance Reports

SapphireIMS has an Advanced Reports feature for ITSM and CMDB modules. This section describes the pre-requisites for this feature.

Ports Availability	The following ports are used by Advanced Reports and needs to be available for binding on the local system where Advance Reports is installed. • 3306 (TCP/UDP) or User Specified Port [Used for communication to SapphireIMS schema in MySQL database server.] • 8761,9001,9002,9003,9005,9006,9007,9008,9099 or User Specified Port
Ports	This is not applicable if the Firewall is disabled. If the Firewall is enabled, the following ports are to be specified in the Exception rules of the Firewall. • 3306 (TCP/UDP) or User Specified Port [**Required only on MySQL Server if MySQL Server is setup on different system**] • 9099 or User Specified Port
Services	The following services should be running, and the services should be configured to start automatically after system restart. • SapphireMySQL or MySQL [In scenarios where MySQL is running on a different system, ensure that the service on the remote server is running] • SapphireIMSAR

15 Log Analyzer

Log analyzer is used to collect and store the log data from different sources like, Event log, SNMP Traps, Syslog, Application logs, NetFlow and sFlow. This section describes the prerequisites for this feature.

Services	The following services should be running, and the services should be configured to start automatically after system restart. • Sapphire ES service • Sapphire Log Analyzer service • SapphireIMS service

Others	Log Analyzer will be available only after you install the SapphireIMS Log Analyzer plug-in. Refer to the document 'SapphireIMS Log Analyzer 5.0 Plug-in Ver 1.5 Installation.pdf' available on 'http:www.sapphireims.com/patches' for the details on installation.

16 NetFlow

SapphireIMS Log Analyzer has capability to monitor the flow data of routers, switches, firewall and gateway devices and to convert that data into charts and tables for easy analysis. SapphireIMS supports the NetFlow protocol for monitoring traffic. SapphireIMS can also generate alerts for data that breach the configured conditions. This section describes the pre-requisites for this feature.

Others	NetFlow will be available only after you install the SapphireIMS Log Analyzer plug-in. Refer to the document 'SapphireIMS Log Analyzer 5.0 Plug-in Ver 1.5 Installation.pdf' available on 'http:www.sapphireims.com/patches' for the details on installation.

17 sFlow

SapphireIMS Log Analyzer has capability to monitor the flow data of routers, switches, firewall and gateway devices and to convert that data into charts and tables for easy analysis. SapphireIMS supports the sFlow protocol for analyzing broad based trends. SapphireIMS can also generate alerts for data that breach the configured conditions. This section describes the pre-requisites for this feature.

Others	sFlow will be available only after you install the SapphireIMS Log Analyzer plug-in. Refer to the document 'SapphireIMS Log Analyzer 5.0 Plug-in Ver 1.5 Installation.pdf' available on 'http:www.sapphireims.com/patches' for the details on installation.

18 Wake on LAN

SapphireIMS provides Wake-on-LAN (WOL) support, an Ethernet computer networking standard that allows a computer to be turned on or awakened by a network message.

SapphireIMS initiates the message transmission through three types of subnet directed broadcasts:

1. Broadcast
2. Directed Broadcast
3. Unicast

This section describes the pre-requisites for this feature.

18.1 Pre-Requisites for End Nodes

Ports	This is not applicable if the Firewall is disabled. If the Firewall is enabled, the following ports are to be specified in the Exception rules of the Firewall. • 7 (UDP)
Notes	• Systems should be WOL enabled in the BIOS for it to accept magic packets. • In SapphireIMS agent environment, the distribution server (Master Agent) should be designated. The 'message push' from a master agent is supported only on Windows.
For Unicast type of broadcast	• Systems from where the packet is unicast must have ARP cache entry (or static ARP cache) of the system to which the packet is sent.

19 General

19.1 Connectivity between MSP Probe and MSP Server

This pre-requisite applies to only the SapphireIMS Enterprise Plus Edition.

The network connectivity between MSP Probe and MSP Server should be a direct connection. The feature is not supported in a proxy or firewall environment because proxy support is not provided in MSP setup.