SapphireIMS 4.0
Product Features

COPYRIGHT NOTICE AND DISCLAIMER

All rights reserved.

No parts of this document may be reproduced in any form without the express written permission of Tecknodreams Software Consulting Pvt. Ltd. Tecknodreams makes no representations or warranties with respect to the contents hereof. In addition, information contained herein is subject to change without notice. Every precaution has been taken in the preparation of this document. Nevertheless, Tecknodreams assumes no responsibility for errors or omissions or any damages resulting from the use of the information contained in this publication.

All trademarks belong to their respective owners.
Introduction

The emergence of new technologies, IT becoming an integral part of the business, periodic churn of IT administrators and mobile work cultures has increased the complexity of IT infrastructure management in today’s world. CIOs must be adequately equipped to handle the challenges posed to them in order to assure the smooth running of their business IT environment. CIOs and IT managers are looking towards implementing proven IT policies to handle these challenges effectively. To implement the processes, integrated and standards compliant products have become the need of the hour.

SapphireIMS is a comprehensive integrated IT infrastructure management suite, with a complete set of features that are needed to manage your organization’s IT infrastructure in an intuitive, efficient and standards compliant manner.
SapphireIMS offers an integrated set of features to help CIOs and IT managers handle the challenges faced by them efficiently and stay in control of their IT environment in a process oriented manner.

SapphireIMS comes with simple, easy to use console and web-based interfaces and simplifies the complexity of management. Executive dashboards provide quick views of the IT environment on a single click.

This document provides the details about the features offered by SapphireIMS. The technical pre-sales team can be contacted for clarifications or further details.

SapphireIMS supports a distributed architecture where the solution can be deployed in a single server or distributed over N servers based on the scalability requirements.

![Diagram of SapphireIMS architecture](image)

**Figure 1**

SapphireIMS remote data collectors or probes are deployed in remote offices for localizing the data collection and the collected data is sent to the central server through a secure HTTP link as shown in Figure 1. This approach optimizes the usage of the WAN bandwidth.

If the scalability demands are high, a distributed approach can be followed with the database installed on a separate server and the application on a separate server and this can be achieved without re-architecting the solution.
SapphireIMS also provides support for unified agent architecture using which devices/systems can be managed seamlessly and all the agents communicate with the central server through web services interface. The communication between the agents, probes and the central server is encrypted and is completely secured.

The probes perform the job of replication agent or port multiplexer as they talk to the central server behalf of the agents running in the local environment.

There is often requirement to support multiple departments in an organization with distinct business processes or in the case of managed service providers to manage IT services for various organizations. This can be achieved using the multi-tenant feature of SapphireIMS which allows the data and processes for each department or organization to be maintained in a secure and independent manner.

SapphireIMS has complete high availability support and the architecture diagram in Figure 2 depicts the same.

![Figure 2](image)

- Failover of Application, System, Network failures
- Microsoft Windows Server 2003 and Microsoft Cluster Server(MSCS)
- External SCSI array connected to both the systems
- Heartbeat using redundant LAN

**Service Desk**

Centralized service desk allows the organization to streamline the service delivery and measure the effectiveness in a qualitative and quantitative manner.
- Industry standard and best practices ITIL templates (Incident management, Problem Management, Change Management and Ad-hoc Service Desk) built-in for direct use

- Ability to publish the standard service delivery offerings as a ‘Service Catalog’ for quick reference.

- Align service delivery mechanism with the organization’s IT service delivery process. Ability to create multiple ‘projects’ for controlled access and project specific configurations

- Configurable service-request state machine flow to enable the organization to achieve the same

- Support for distinct work-flows for administrators/technicians and external users

- Ability to synchronize with Active Directory / LDAP

- Associate service-request with Locations and Departments

- Associate service-request with Categories, Sub-categories, Criticality, Severity and other relevant fields to provide complete information about it in a simplified manner

- Configurable interfaces to populate standard fields (Location, Department, Category, Sub-category, Severity) to simplify the service-request submission process

- Support for dynamic fields / context sensitive fields based on service request category

- Support for dynamic enclosure additions to provide meaningful information about the service requests

- Ability to add attachments as part of service requests

- Support for multiple source for service request logging
  - Email
  - Web
  - Telephone (Manual entry created by the administrator on behalf of the user)

- Associate approval control with service-requests. Enables the organization to control specific service-requests to get approved from the approval authorities. Example: Licensed software installation requests need approval from the approval authority

- Configurable Automatic Assignment algorithm for assigning service-requests to the administrators
• Integration with SMS sub-system for generating SMS alerts to notify the administrators

• Knowledge base
  o Support for approval mechanism to store the appropriate details.
  o Search on the contents and managing the same

• SLA Monitoring
  o Assign service delivery time as per organizations process based on nature of service requests.
  o Assign escalation mechanism
  o Support for suspended states of request processing to have more accurate SLA as per the organization process definition
  o SLA engine monitors each service request against the expected service delivery time. Upon violation, escalated to right users to bring it to management visibility.

• Maintenance of History for auditing purpose

• API’s for automatic submission of service requests from fault management and other IMS modules

• Interface to schedule ticket submission for routine jobs (weekly backups etc)

• Interface to automatically convert the email received as a service request or to maintain an email queue internally

• Notifications through E-Mail/SMS

• Interface to broadcast critical information through service desk ‘Announcements’

• Ability to conduct online surveys to collect end user feedback

• Reports
  o SLA Compliance Report
  o User-wise call status Report
  o Administrator call status Report
  o Statistical reports using any of the service desk parameter
  o Trends
    ▪ Call Arrival
    ▪ Call Resolution

• Powerful filters for ease-of-use

• Automation layer – Helps to perform conditional call routing to specific roles in the system based on the business rules provided
• Scripting layer – Ability to launch pre and post action scripts specific to the context of the request thus providing tighter integration within different modules as well as 3rd party applications.

Asset lifecycle management

Asset information like make/model/hardware details/ warranty details/ PO details etc for each of the asset type can be modeled and captured. This can be reconciled and tagged with the discovered inventory. The entire asset life cycle operations (right from procurement to scrap) can modeled and linked with the service desk, thereby there won’t be any asset movement/ allocation without a valid service request. Organizations can also have an up to date record of who uses what and also the in stock items of the inventory thus making planned procurements.

System supports inventory and change management for heterogeneous IT environment. The standard based data collection approach helps the organization to keep the dynamic inventory information reflecting the current state.

- Modeling of assets and associated properties as per your business need (make/warranty details/ purchase details/ vendor details etc). System provides asset of built-in asset templates and also the ability to add custom fields as per user needs. No restriction on the number of fields.

- Configurable asset life cycle state machine (Procurement till retirement), allows you to stay in complete control of assets (who uses what asset and where)

- Auto Discovery
  - Auto enumeration of Windows devices
  - Network Devices & Servers
  - Configuration
    - Discovery interval
    - IP range
    - Windows Domains

- Agents can be pushed to the target systems through Agent distribution engine which is available for domain environments.

- Detailed System / Device Inventory
  - System, Bios, Disk, CPU, Memory, Interface configuration, User Configuration, Ports, Installed Software, Peripherals, Hot-fixes, Serial numbers, etc.

- Ability to monitor heterogeneous systems(Windows XP, Windows 7, Windows 2003 Server, Windows 2008 Server, Linux, AIX, HP-UX, Solaris) using the
standard based approach. Supported standards are

- Windows Management Interface (WMI)
- Simple Network Management Protocol (SNMP v1/ v2c, v3)
- Web Based Enterprise Management (WBEM)
- SSH

- Discover changes in the base-lined inventory
- Mapping between the locations and systems/devices
- Ability to add custom-tags, inventory item number, etc.
- Ability to add external custom depreciation rules
- Ability to associate discovered system with additional fields like an inventory-tag, Warranty period, AMC period, Service provider, etc.
- Support for maintaining non-digital / un-managed IP inventory
- Reports
  - Multiple format support – PDF, Excel, HTML
  - Overall inventory
  - Software inventory
  - Hardware inventory

**Software License Management**

Effective vigil against the license usage is must to save the cost as well as to avoid license violations.

- Master License inventory to hold the existing licenses purchased from various vendors; Ability to add the licenses as per the purchase models with an ease to map to Purchase orders
- Support for time-based and permanent licensing approaches
- Dynamically retrieved software inventory in the organization
- License installation analysis and Reporting
- Violation reports along with the installation details enabling organization to quickly act and be compliant all the time

**Policy Management**

SapphireIMS helps the organizations to perform effective IT policy audit of their existing infrastructure against well derived organization policies.
- Mapping of organization IT policies into SapphireIMS policy rules
- Support for multiple policies
- Logical mapping of policies and the systems expected to comply
- Easy generation of compliance and non-compliance reports

**IMAC Process Implementation / Service desk Integration**

Seamlessly integrates with SapphireIMS Service desk to deliver the following features.

- Logging of service requests/incidents/problem/change against the assets or CI’s. Enables the tracking of chronic assets, repeated issues, etc.
- Asset lifecycle management (IMAC) process implementation which ensures that the assets are managed as per the defined process and also updates the asset repository automatically to keep the records intact
- Can be extended to include asset allocation management processes which may involve one or more approvals

**System Management and Automation**

System Management automation includes tasks that would be repetitive in each Windows system and would require a desktop visit in the normal scenario. SapphireIMS provides a framework using which these tasks can be automated and scheduled and executed as a batch. This ensures that the remote tasks get completed on the target systems without a desktop visit, ensuring a faster and controlled execution. The following list explains the set of activities that are available as part of the framework

- **Patch Management**
  - Helps to scan the network for all the missing windows patches
  - Allows administrators to perform a patch approval, upon which the patch gets downloaded and deployed in the target devices
  - Central Management of all the windows patches, provides control of critical patches and also saves bandwidth

- **Share Management** - Manage all the open shares and the properties on the network

- **Managing External Drives** - Enable/Disable external drives on the target systems remotely, Drives include Floppy/ CD Drive and USB drives
- User account management - Manage User accounts and the privileges set for them remotely (operation includes all standard user account settings as provided by Windows)

- Executing any Custom Script - Launch scripts remotely on the target systems

- Disk Management - Perform disk management activities like fragmentation remotely and periodically

- Managing Environment Variables - Manage environment variables and their properties remotely (operation includes both the system and user variables)

- IE Proxy Setting - Deploy IE proxy setting properties to all target browsers. This helps in controlling and managing the setting.

- Software Installations - Deploy software packages remotely; also uninstall restricted software remotely if it is detected in the network

- Printer deployment - Manage the printer additions and deletions remotely. This helps when a new printer gets deployed in the network and the same can be configured in the target devices.

- System Restore - Manage the system restore settings (turning off or turning on) as per the IT policy of the network.

- USB Port(s) - Manage the usage of USB data drive policy (example disabling the usage of USB data drives to be used in the network, and selectively enabling it on need basis)

**System Maintenance activities**

System Maintenance activities include periodic or ad-hoc maintenance activities that would need to be carried out on the target devices. This includes

- Shutdown devices
- Reboot devices
- Power On devices (if in case Wake-On LAN feature is enabled)

**Business Service Monitoring**

Organizations are aware that even a marginal downtime is enough to impact their revenue margins by virtue of lesser productivity or in some cases even lost business opportunities.

A common myth is that business continuity assurance is about having a process by which plans are put in place and managed to ensure that IT Services can recover and continue should a serious incident occur. It is not just about reactive measures, but also about proactive measures - reducing the risk of a disaster in the first instance. As organizations grow in size there is an exponential increase in the IT adoption to
improve business efficiency. SapphireIMS supports monitoring of the performance and health of Critical servers, applications and links. Performance monitoring is critical to assure business continuity and capacity planning.

- System level data collection interval support
- No custom/proprietary agents needed for data collection
- Ability to monitor heterogeneous systems (Windows 9x/2000/XP/7/2003/2008, Linux, Solaris, AIX, HP-UX) using the standard based approach. Supported standards are
  - Windows Management Interface (WMI)
  - Simple Network Management Protocol (SNMP)
  - Web Based Enterprise Management (WBEM)
  - SSH
- Standard performance Parameters
  - CPU
  - Disk
  - Interface
  - Memory
  - Paging
  - Disk I/O
  - Device/vendor specific parameters (for instance, printer monitoring supports the number of pages printed, toner details etc, UPS monitoring supports the battery health, CISCO devices provides cisco specific health monitoring parameters)
- Plug-in support for IPSLA monitoring
- Availability monitoring
  - System
  - Interface
  - Application
  - Windows Services and processes
- Supports threshold monitoring of the parameters collected
  - Configuration
    - Value range for the parameters to raise ‘Information’ alert or ‘Warning’ alert or ‘Error’ alert
    - Enabling / Disabling of consecutive alerts for recurring problem
    - Tolerance level to indicate the acceptable time-limit for each problem
Alarms and Alerts are generated upon threshold breach and following actions can be configured:

- E-mail alerts based on roles or users
- SMS alerts based on roles or users
- Launching of custom applications
- Service Desk ticket creation

- Historical data storage

- Reports
  - Intuitive graphs to indicate collected parameter value performance
  - TopN reports and Business Intelligence Reports
  - Historical data based
  - Multiple format support – PDF, HTML
  - Automatic mailing of reports as per the configuration

**Business level Monitoring**

Traditionally organizations monitor infrastructure components, applications, services, etc. separately and take corrective actions. As the business service delivery infrastructure complexity grows with the adoption of cloud, etc., it becomes critical to monitor the health and availability from the service perspective which has direct impact over business.

SapphireIMS allows the organization to define business critical services and their dependent infrastructure components with redundancy, impact, etc. It provides intelligent notifications upon threshold breach which helps the service personnel to act quickly to avoid any degradation in service performance and avoid potential disasters.

**Service Quality Monitoring / Synthetic Transactions**

SapphireIMS has an ability to measure the service quality of the business applications which are critical to the organization. Monitoring availability does not give enough details about the end-user experience and measuring the actual service quality by performing synthetic transactions helps to get a better view.

- Supports services quality monitoring of
  - E-mail
  - FTP Services
  - HTTP
  - DNS
  - RADIUS
  - DHCP

- Parameters are collected by performing synthetic transactions. Hence, collected parameters reflects actual user experience for the same services
• Supports thresholds monitoring of the service quality parameters
  
  o Configuration
    ▪ Service quality parameter value range
    ▪ Enabling / Disabling of repeated alerts for recurring problem
    ▪ Tolerance level to indicate the acceptable time-limit for each problem
  
  o Alarms and Alerts are generated upon threshold breach and following actions can be configured
    ▪ E-mail alerts based on roles or users
    ▪ SMS alerts based on roles or users
    ▪ Launching of custom applications
    ▪ Service Desk ticket creation
  
  o Historical data storage

• Reports
  
  o Intuitive graphs to indicate collected parameter value performance
  o Historical data based
  o Multiple format support – PDF, HTML
  o Automatic mailing of reports as per the configuration

**Network Device & Link Monitoring**

SapphireIMS has an ability to monitor critical devices and utilization of the backbone links.

• Discovers the devices in the network; Complete support for heterogeneous multi-vendor environment

• No custom/proprietary agents needed for data collection

• Ability to monitor devices using the standard based approach. (SNMP)

• System supports the polling of Enterprise MIB to find out the device classification. If the device is not supported by default, it can be discovered through additional configuration based on IETF/RFC standard MIBs published by the equipment manufacturer.

• SNMP Traps and Syslog event collection

• Interface statistics

• Supports threshold monitoring of the parameters collected
  
  o Configuration
- Value range for the parameters to raise ‘Information’ alert or ‘Warning’ alert or ‘Error’ alert
- Enabling / Disabling of consecutive alerts for recurring problem
- Tolerance level to indicate the acceptable time-limit for each problem
  - Alarms and Alerts are generated upon threshold breach and following actions can be configured
    - E-mail alerts based on roles or users
    - SMS alerts based on roles or users
    - Launching of custom applications
    - Service Desk ticket creation

- Historical data storage

- Systems/Devices can be configured for scheduled maintenance and this shall take care of avoiding generating alarms and notifications during the planned maintenance period.

- Role based User access control to limit the access to critical devices and views

- Reports
  - Intuitive graphs to indicate collected parameter value performance
  - Historical data based
  - Multiple format support – PDF, HTML
  - Automatic mailing of reports as per the configuration

**Application Health Monitoring**

SapphireIMS has built-in mechanism to monitor the health of popular applications in the market.

- Currently supported applications include
  - Database servers (MySQL, MS*SQL, Oracle, Sybase)
  - Application servers (Tomcat, JBoss)
  - Microsoft Applications (IIS, Active Directory, Exchange Server)

- Ability to monitor heterogeneous systems using the standard based approach. Supported standards are
  - Windows Management Interface (WMI)
  - Custom scripts
  - Java Management Extensions (JMX)

- Plug-In development interfaces are available to add the health monitoring for other standard / custom applications
• Alarms and Notifications are generated upon threshold breach and the following actions can be configured.
  - E-mail alerts based on roles or users
  - SMS alerts based on roles or users
  - Launching of custom applications
  - Service Desk ticket creation

• Historical data storage

• Reports
  - Intuitive graphs to indicate collected parameter value performance
  - Historical data based
  - Multiple format support – PDF, HTML
  - Automatic mailing of reports as per the configuration

**Event Collection & Management – Log Analyzer**

SapphireIMS has an ability to collect and analyze critical logs and events generated by the critical servers and devices.

• Supported log-types
  - Windows Event logs
  - SNMP Trap messages
  - Syslog messages
  - Application logs (file based)

• Retrieval is instantaneous in case of SNMP Traps and Syslogs

• Retrieval of Event Logs is incremental for as per the configured interval

• Supports a rule based engine to convert the collected events and logs to alarms and generate notifications.
  - Flexible Rule Configuration. Rule can be defined based on
    - Log type Event Logs/ SNMP Traps/ Syslog
    - Facility
    - Application generating the log

  - Alarms and Alerts are generated based on the rule defined
    - E-mail alerts based on roles or users
    - SMS alerts based on roles or users
    - Launching of custom applications
    - Service Desk ticket creation

  - Historical data storage
• Presentation
  o Historical data based
  o Multiple format support – PDF, HTML, Excel