NOKIA

NSP
Network Services Platform

Release 19.3

System Architecture Guide

3HE-15139-AAAA-TQZZA

Issue 1

March 2019

Legal notice

Contents

About this document

Purpose

The *NSP System Architecture Guide* describes the Network Services Platform architecture and interoperation with other systems from a high-level perspective. The audience is a technology officer, network planner, or system administrator who requires a broad technical understanding of the NSP system structure and design methodology.

The guide scope is limited to a description of the integral elements that are common to NSP components. For information about the architecture of a specific NSP product module other than the NSD and NRC modules, or a product or appliance that integrates with the NSP, see the associated documentation.

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

Documentation feedback

1 About the NSP

1.1 NSP product description

1.1.1 The NSP system

The Network Services Platform, or NSP, is a network management system that provides traditional and Software Defined Networking, or SDN, service management functions across multiple network domains. The NSP provides interfaces that enable network operators to perform multi-layer service preconfiguration, rollout, and activation. The NSP can deploy and manage services that employ multiple technologies and span network domains such as IP/MPLS, optical, and wireless.

The NSP also manages the physical and virtual network infrastructure, including equipment from third-party vendors.

The NSP can integrate IP/MPLS and optical management platforms using carrier SDN technology to:

- accelerate the creation and rollout of on-demand IP/optical network services
- enable real-time service optimization and flow steering
- extend assurance capabilities and automates assurance functions

1.1.2 Design ideology

The NSP incorporates design considerations that include:

- open standards that promote interoperation with third-party management systems
- modular, flexible internal architecture to accommodate new functions
- deployment flexibility for adaptation to changing network management scope or complexity
- centralized, proprietary nspOS resource base for system components
- centralized web services and single sign-on, or SSO, access to NSP applications
- distributed processing for efficiency and horizontal scalability
- redundant component deployment and other fault-tolerance mechanisms
- stringent security between components
- secure local and remote client access

1.1.3 NSP Launchpad

The browser-based NSP Launchpad is the graphical operator interface that provides access to all licensed NSP applications. You can also use the Launchpad to open other applications and traditional management interfaces, gain access to user documentation, and perform basic system administration. Some NSP applications support the cross-launch of other applications.

1.2 NSP system components

1.2.1 Overview

An NSP system may include multiple components that are deployed as separate processing entities, depending on the network management scope and deployment complexity.

The principal elements of an NSP system are called modules. An NSP system may include other products, ancillary devices, or appliances, which together with the NSP modules in an NSP system are, for simplicity, called the NSP system components.

NSP modules

NSP modules are the orderable commercial units that comprise the NSP product:

- Network Services Director, or NSD
  - SDN L2 and L3 service fulfillment
  - Assurance using service supervision
  - Model-driven mediation of Nokia and multi-vendor devices
- Network Resource Controller - Cross-domain, or NRC-X
  - IP/optical traffic correlation
  - Cross-domain link creation and discovery
- Network Resource Controller - Packet, or NRC-P
  - IP/MPLS network optimization
  - IP/MPLS path computation
  - Flow steering based on statistics, analytics, and operator action
- Network Functions Manager - Packet, or NFM-P
  - IP/MPLS network infrastructure management
  - IP/MPLS network and service assurance
  - Traditional L2 and L3 service management

Other system components

An NSP system can also include other products, components and appliances that include the following:

- Network Functions Manager - Transport product, which is required for optical management functions
- Network Resource Controller - Transport, or NRC-T, an IP/MPLS and optical management-system mediator product required for NSP and NFM-T integration
- Virtual Service Router - Network Resources Controller, or VSR-NRC, which acts in a Virtual Network Function, or VNF, capacity to perfom topology discovery
- vCPAA, which performs control-plane assurance analysis and reporting
- MDM, which provides model-driven mediation of network elements, or NEs
- CLM, which provides centralized NE license management
- NSP analytics servers, which use business-intelligence software to generate reports about network conditions and trends for the NSP Analytics application

- NSP Flow Collectors, which collect Cflowd statistics from NEs for processing by third-party tools, or for report generation by NSP analytics servers
- Flow Collector Controllers, which manage NSP Flow Collectors

1.2.2 Independent and shared-mode deployment

You can deploy an NSP module as an independent system, or in combination with other components to create a shared-mode deployment that expands the NSP network management capabilities. See the *NSP Deployment and Installation Gudie* for information about the supported deployment scenarios.

1.2.3 nspOS common resource base

The nspOS is a set of embedded platform services that is required by each NSP component. The nspOS provides central session management functions and services such as SSO access, application cross-launch, and operator access to applications from the NSP Launchpad.

The nspOS services and functions include the following:

- **Login**—grants SSO access to all NSP applications, GUI clients, and other resources on the NSP Launchpad
- **NSP Launchpad**—entry point for all NSP applications
- **Central Authentication Server, or CAS**—authenticates user login attempts
- **Session Manager**—tracks and manages SSO sessions
- **REST API Gateway**—acquires NSP REST API tokens and locates specific NSP APIs

The nspOS also contains a service registry, distributed streaming platform, and graph database.

1.3 Network management functions

1.3.1 Overview

The NSP provides a comprehensive suite of browser-based applications for various network management functions.

1.3.2 Service deployment and assurance

The NSP SDN functions enable dynamic, rapid customer service rollout and validation. Each service can be monitored to provide performance, usage, and fault information. Applications such as Service Supervision, Fault Management, Link Utilization, Network Supervision, and Wireless Supervision provide information to assist in the timely apprehension, troubleshooting, root-cause analysis, and correction of network and service issues.

1.3.3 Traffic optimization

Applications such as Traffic Scheduler, Traffic Steering Controller, and IP/MPLS Optimization automate traffic management by controlling and steering traffic flows as specified by a network operator.

1.3.4 Performance KPI monitoring and reporting

The NSP monitors network KPIs for immediate and trend-based reporting by NSP applications. The reporting agents include the NSP Telemetry application, which receives near-real-time NE KPIs, and NSP Analytics, which uses raw and aggregated flow statistics for long-term reporting to identify trends and potential capacity issues.

1.3.5 Equipment inventory management

For some functions, the NSP draws upon modules such as the NFM-P, which maintains a dynamically updated network equipment data store for NSP applications such as Inventory Management.

An NSP system that includes the MDM enables the Device Administrator and Modeled Device Configurator NSP applications for managing a network equipment inventory using model-driven mediation.

1.3.6 Administrative and monitoring functions

Applications such as the NSP Workflow Manager, Policy Management, and Supervision Manager simplify network administration. The NSP Service Navigator, Wireless NE View, and Subscriber Manager provide real-time views of network and service objects.

2 System structure

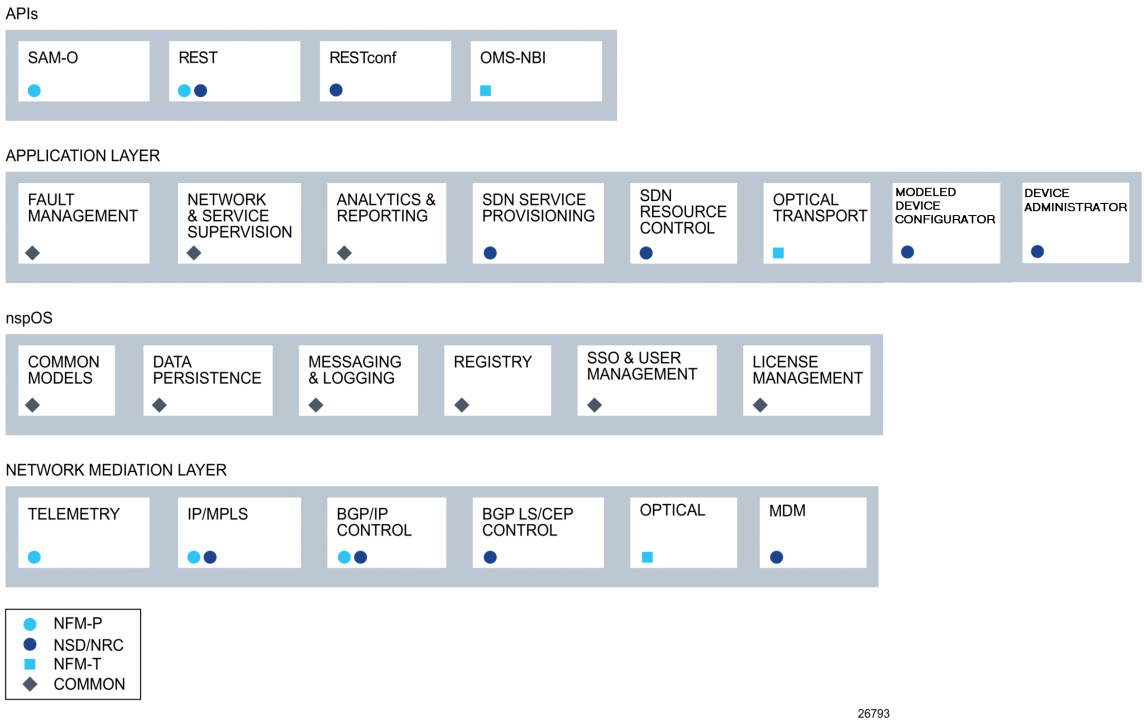
2.1 Core NSP system elements

2.1.1 Description

The modular NSP architecture is readily adaptable to changing management needs, and simplifies the transition to SDN for 5620 SAM and 1350 OMS customers. The architecture allows for system expansion and the addition of network functions as required.

The following figure shows a high-level view of the core NSP functions as a layered architecture model.

Figure 2-1 Core NSP functions, layered view



2.2 Central management functions

2.2.1 Network data management and correlation

The NSP uses a Neo4j graph database to identify relevant connections between network events and operator actions in order to maintain awareness of network conditions. Neo4j is the engine behind NSP assurance applications such as Fault Managment.

The NSP PostgreSQL database adds intelligent integration and interpretation functions to identify complex network data relationships, and provides input to NSP applications for functions such as root-cause analysis.

2.2.2 Network state synchronization and event notification

The NSP uses the Kafka messaging subsystem, a subscription-based distributed streaming platform, to synchronize network and operational information among NSP components, and to send network event notifications to OSS consumers that subscribe to NSP Kafka topics.

2.2.3 NSP REST API

The NSP REST API is an abstracted interface for application developers can use to provision and monitor network objects, and to subscribe to real-time network event notifications. The REST API supports SDN, service assurance, and IP/MPLS and optical network managment functions.

2.2.4 ZooKeeper registration service

The NSP ZooKeeper registration service maintains a repository of information about each NSP component, and controls access to the active nspOS instance through which each component gains access to the common NSP resource base of platform services.

3 Security

3.1 Overview

3.1.1 TLS

NSP interfaces are secured using Transport Layer Security, or TLS, which is implemented using an NSP PKI server or customer-provided certificates.

Session credentials and messages are protected using mechanisms and protocols that include the following:

- HTTPS, as the application-layer transport for API clients
- SNMPv3, for secure SNMP communication with the managed network
- NAT, at the network layer, between system components

3.1.2 Session management

Effective session management requires authentication, authorization, and accounting, or AAA.

- Local NSP authentication is performed using a local security scheme and user database.
- The supported third-party authentication methods include RADIUS, TACACS+, LDAP, SAM-L, and CSA.

Client sessions

All application and API client sessions are authenticated by the NSP central authentication service, or CAS.

3.1.3 Network transport security

Transport-layer security is available to the network protocols that carry messages between NSP components.

3.1.4 Firewall support

The NSP supports firewall deployment on all NSP server interfaces, as described in the *NSP NSD and NRC Planining Guide*. Firewall support among elements of individual component systems may vary. A module such as the NFM-P, or a product such as the NFM-T, may have firewall restrictions on specific interfaces between system elements. See the module or product Planning Guide for information.

3.1.5 NSP data privacy

The NSP protects the network and user data that it collects or processes.

Appendix A, “NSP data privacy summary” describes the mechanisms that the NSP uses for private data collection, storage, security, and retention.

4 NSP fault tolerance

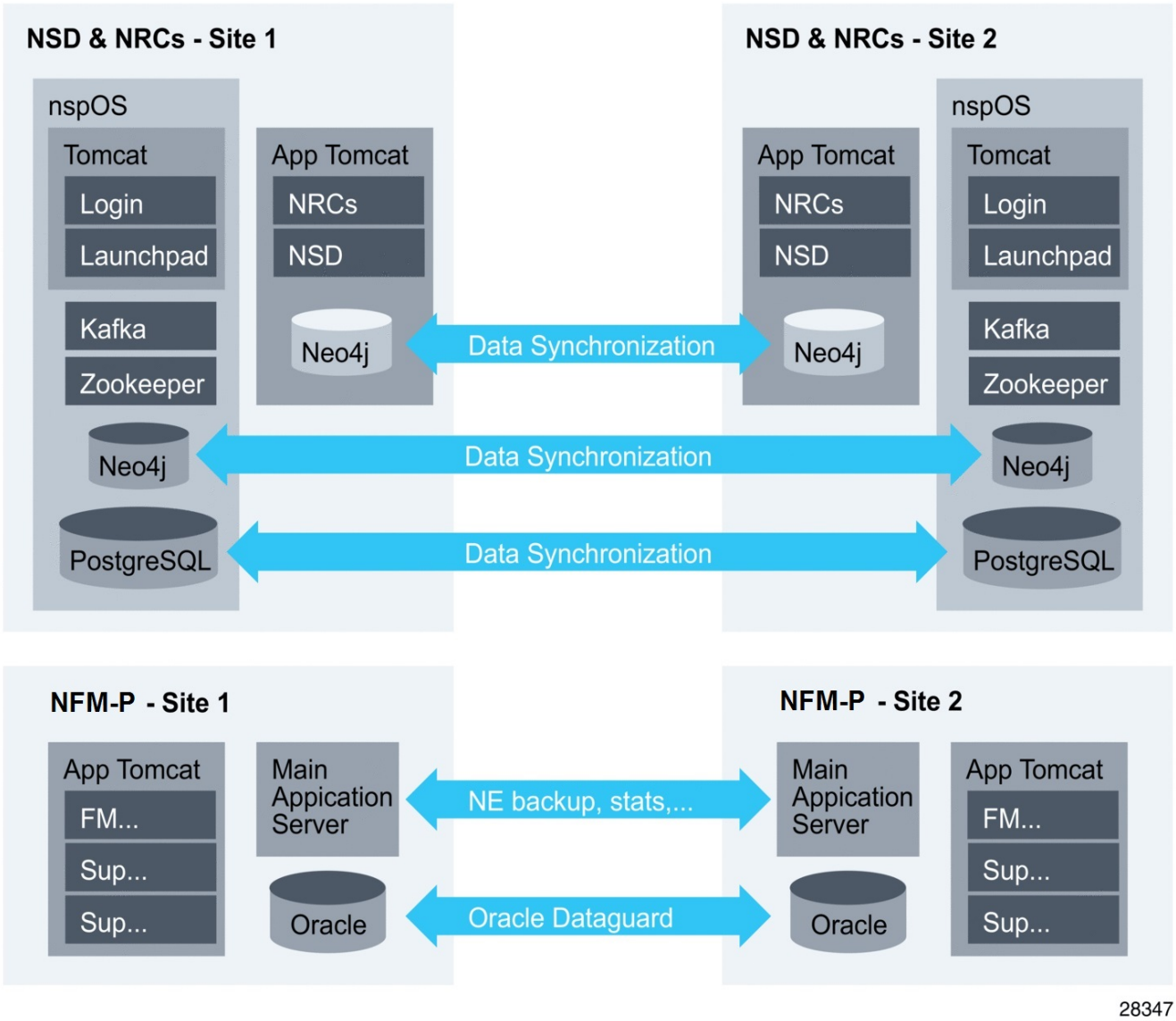
4.1 Overview

4.1.1 Component redundancy

All NSP modules support a 1+1, or warm standby, redundancy model. In such a model, each module has a group of active components, and a group of warm standby components; each component is a separate OS instance that hosts a module function. For example, the NFM-P has main server, main database, and optional auxiliary components. Each main or auxiliary component supports redundant deployment. All active components of a module require low network latency, so ideally are geographically collocated.

See the *NSP System Administrator Guide* for information about the supported redundancy models and redundancy failure and recover scenarios.

The following figure is a high-level example of a geographically redundant NSP system that illustrates the data synchronization between components.



4.1.2 Other fault-tolerance mechanisms

Some components employ fault-tolerance mechanisms in addition to component redundancy.

For example, you can configure an NSP Flow Collector to transfer collected statistics files to redundant remote targets. For a higher degree of fault tolerance, you can configure two or more NSP Flow Collectors to collect statistics from the same set of NEs and transfer the statistics files to redundant destinations. Such a configuration ensures that the statistics collection and transfer continue uninterrupted in the event that an NSP Flow Collector and a transfer destination are each unreachable.

NSP analytics servers use the following additional fault-tolerance mechanisms to ensure that there is no single point of failure or unavailability:

- multiple analytics servers and a load-balancing algorithm that specifies, by turns, which server responds to an Analytics application report request
- access to each station in a multi-station data source, which ensures access to data when a database station is unavailable

A NSP data privacy summary

A.1 NSP network and user data privacy

A.1.1 Purpose

This appendix summarizes how the NSP treats the network and NSP user data that it collects, processes, or retains. The following data categories are described:

- local user authentication data
- NE data
- subscriber data
- e-mail notification policy data

See A.1.2 “NSD and NRC data privacy” (p. 17) for data treatment specific to the NSD and NRC.

SeeA.1.3 “NFM-P treatment of private data” (p. 19) for data treatment specific to the NSD and NRC.

A.1.2 NSD and NRC data privacy

The following table lists and describes, by data category, how the NSD and NRC treats network and user data.

Table A-1 NSD and NRC treatment of private data

Data category	Description and treatment
Local user authentication data	
Type	• Username and password • IP address
Purpose	• Authentication of local NSP users • IP address provides accountability of individual product access.
Storage	• Local database • Logs
Retention	Data is retained in the database until an authorized user deletes it. Log retention time can vary based on log file size and the number of log backups.
Processing	Local user data is processed for the stated purpose.
Access	Authorized users

Table A-1 NSD and NRC treatment of private data (continued)

Data category	Description and treatment
Safeguards	• Additional local users must be created by an authorized user. • Database access is restricted to authorized users. • TLS secures data in transit. • Passwords for local users are hashed before they are stored. • Log file access is restricted to authorized users.
Comments	Local authentication is performed using a local database of users and a local security scheme.
NE data	
Type of data	• Username and password • IP address
Purpose	• NE authentication • NE IP address for NE discovery/access
Storage	• Local database • Logs
Retention	Data is retained in the database until an authorized user deletes it. Log retention can vary based on the log file size and number of log backups.
Processing	NE data is processed for the stated purpose.
Access	Authorized users
Safeguards	• NEs are configured by authorized users. • Database access is restricted to authorized users. • Secure transit option is available. • Passwords for NE users are encrypted before being stored. • Log file access is restricted to authorized users.
Subscriber data	
Type of data	• MAC address • IP address
Purpose	• Statistics • SLA compliance • Troubleshooting
Storage	• Local database • Logs
Retention	Data is retained in the database until an authorized user deletes it. Log retention can vary based on the log file size and number of log backups. Retention period for statistics can be configured.
Processing	Subscriber data is processed for the stated purpose.

Table A-1 NSD and NRC treatment of private data (continued)

Data category	Description and treatment
Access	Authorized users
Safeguards	• NEs are configured by authorized users. • Database access is restricted to authorized users. • Log file access is restricted to authorized users.
E-mail notification policy data	
Type of data	• Username and password • E-mail address (sender) • E-mail address (recipient)
Purpose	• Username, password and sender's e-mail address are used for SMTP configuration • Recipient e-mail addresses are required to create e-mail notification policies in supported applications (for example, Fault Management application for alarm notifications)
Storage	• Local database
Retention	Data is retained in the database until an authorized user deletes it. By default, SMTP server and application e-mail notification policies are not configured.
Processing	SMTP server configuration and application e-mail notification policies are processed for the stated purpose.
Access	Authorized users
Safeguards	• SMTP configuration and application e-mail policies are configured by authorized users. • Database access is restricted to authorized users. • Password for SMTP configuration is encrypted before being stored.

A.1.3 NFM-P treatment of private data

The following table lists and describes, by data category, how the NFM-P treats network and user data.

Table A-2 NFM-P data privacy

Category	Description
Local user data (local authentication)	
Type of data	• Username and password • E-mail • IP address

Table A-2 NFM-P data privacy (continued)

Category	Description
Purpose	• Authentication of local NSP users • User e-mail addresses (optional) to send notifications for certain events; for example, alarms or account status • IP address provides accountability of individual product access.
Storage	• Local database • Logs
Retention	Data is retained in the database until an authorized user deletes it. Log retention time can vary based on log file size and the number of log backups.
Processing	Local user data is processed for the stated purpose.
Access	Authorized users
Safeguards	• Additional local users must be created by an authorized user. • Database access is restricted to authorized users. • TLS secures data in transit. • Passwords for local users are hashed before they are stored. • Log file access is restricted to authorized users.
Comments	Local authentication is performed using a local database of users and a local security scheme.
Customer profile data	
Type of data	• Name • E-mail • Address • Phone
Purpose	Data may be used by an authorized user for associating customers to configured services.
Storage	Local database
Retention	Data is retained in the database until an authorized user deletes it.
Processing	Customer profile data is processed for the stated purpose.
Access	Authorized users
Safeguards	• Customer profile must be created by an authorized user. • Database access is restricted to authorized users.
NE data	
Type of data	• Username and password • IP address
Purpose	• NE authentication • NE IP address for NE discovery/access

Table A-2 NFM-P data privacy (continued)

Category	Description
Storage	• Local database • Logs Note that NE backups that are stored on the NFM-P server may contain data that is not stored in the NFM-P database. Data contained in the NE backup files will be dependent upon the NE type and version; therefore the privacy statements for the individual NEs should be consulted.
Retention	Data is retained in the database until an authorized user deletes it. Log retention can vary based on the log file size and number of log backups.
Processing	NE data is processed for the stated purpose.
Access	Authorized users
Safeguards	• NEs are configured by authorized users. • Database access is restricted to authorized users. • Secure transit option is available. • Passwords for NE users are encrypted before being stored. • Log file access is restricted to authorized users.
Subscriber data	
Type of data	• MAC address • IP address • International Mobile Subscriber Identity (IMSI) • International Mobile Station Equipment Identity (IMEI) • Mobile Station International Subscriber Directory Number (MSISDN) • Access Point Name (APN)
Purpose	• Statistics • SLA compliance • Troubleshooting • Analytics • UE or network node performance information
Storage	• Local database • Logs • Auxiliary collector servers (optional): statistics, PCMD, and call trace • Analytics server (optional)
Retention	Data is retained in the database until an authorized user deletes it. Log retention can vary based on the log file size and number of log backups. Retention period for auxiliary servers can be configured.
Processing	Subscriber data is processed for the stated purpose.
Access	Authorized users

Table A-2 NFM-P data privacy (continued)

Category	Description
Safeguards	• NEs are configured by authorized users. • Database access is restricted to authorized users. • Secure transit option is available. • File access is restricted to authorized users. • Log file access is restricted to authorized users.
E mail notification policies	
Type of data	• Username and password • E-mail address (sender) • E-mail address (recipient)
Purpose	• Username, password and sender's e-mail address are used for SMTP configuration • Recipient e-mail addresses are required to create e-mail notification policies in supported applications (for example, Fault Management application for alarm notifications)
Storage	• Local database
Retention	Data is retained in the database until an authorized user deletes it. By default, SMTP server and application e-mail notification policies are not configured.
Processing	SMTP server configuration and application e-mail notification policies are processed for the stated purpose.
Access	Authorized users
Safeguards	• SMTP configuration and application e-mail policies are configured by authorized users. • Database access is restricted to authorized users. • Password for SMTP configuration is encrypted before being stored.