The ISO 20000 *guide*

ManageEngine

Table of contents

Disclaimer

How ManageEngine can help you in complying with the ISO 20000 standard

ManageEngine's comprehensive suite of IT management solutions encompasses tools that can help your organization effectively fulfill the requirements for ISO 20000 compliance. These tools will help you easily integrate the mandated processes as per the ISO 20000-1:2018 requirement document in your organization's operations, and generate evidence necessary for conformance.

Regulations and certifications that ManageEngine products comply with:

ManageEngine solutions comply with a number of standards and certifications including:

ISO/IEC 27001:

One of the most widely recognized independent international security standards. ManageEngine has earned ISO/IEC 27001:2013 certification for Applications, Systems, People, Technology, and Processes.

SOC 2 Type II:

An evaluation of the design and operating effectiveness of controls that meet the AICPA's Trust Services Principles criteria.

GDPR:

A pan-European regulation that requires businesses to protect the personal data and privacy of EU citizens for the processing of their personal data.

ISO/IEC 27017:

The information technology, security techniques, and code of practice for information security controls based on ISO/IEC 27002 for cloud services, a standard that gives guidelines for information security controls applicable to the provision and use of cloud services.

ISO/IEC 27018:

A standard that establishes commonly accepted control objectives, controls, and guidelines for implementing measures on safeguarding the PII that is processed in a public cloud. ISO/IEC 27018 provides guidance to organizations concerned about how their cloud providers are handing personally identifiable information (PII).

ManageEngine products that help in ISO 20000 compliance:

- **ServiceDesk Plus:** Full-stack ITSM suite

- **Analytics Plus:** An on-premises reporting and business intelligence solution

- **OpManager Plus:** An integrated network performance management solution

- **Applications Manager:** A server and application performance monitoring solution

- **Log360:** A comprehensive security information and event management tool

- **PAM360:** A comprehensive privileged access management (PAM) solution

- **AD360:** An integrated identity and access management (IAM) solution

- **Endpoint Central:** A unified endpoint management (UEM) solution

Process requirement mapping

This section elaborates on how ManageEngine solutions can help your organization support different processes mentioned under various clauses in the ISO 20000-1

SERVICE MANAGEMENT SYSTEM (SMS)

Customers (Internal & External)

Services

Service Requirement

Context of the organization
• Organization and its context
• Interested parties • Scope of the SMS
• Establish the SMS

Leadership
• Leadership & Commitment • Policy
• Roles, Responsibilities and Authorities

Planning
• Risks and Opportunities
• Objectives • Plan the SMS

Support of the SMS
• Resources • Competence • Awareness
• Communication • Documented Information
• Knowledge

Operation of the SMS

Service portfolio
• Service Delivery
• Plan the Services
• Control of parties involved in the service lifecycle
• Service Catalogue management
• Asset management
• Configuration Management

Operational planning & Control

Relationship & Agreement
• Business relationship management
• Service level management
• Supplier management

Supply & Demand
• Budgeting & Accounting for services
• Demand Management
• Capacity Management

Service Design, Build & Transition
• Change Management
• Service Design and Transition
• Release & Deployment management

Resolution and fulfilment
• Incident Management
• Service Request Management
• Problem Management

Service assurance
• Service Availability Management
• Service Continuity Management
• Information Security Management

Performance evaluation
• Monitoring, Measurement, Analysis & Evaluation
• Internal Audit   • Management Review
• Service Reporting

Improvement
• Nonconformity and Corrective Action
• Continual Improvement

The mandatory requirements mentioned in ISO 20000-1 that need to be fulfilled for certifica-
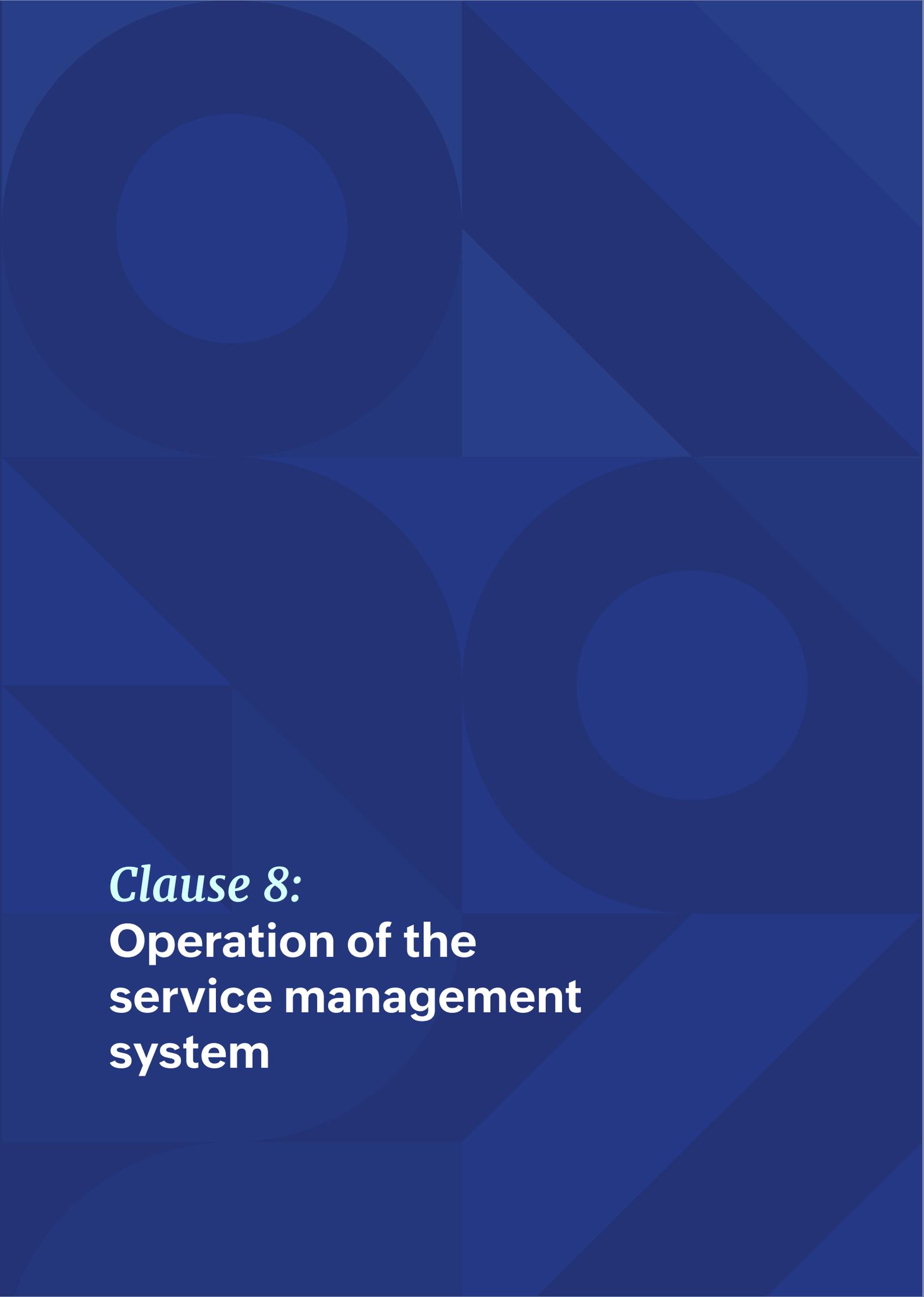
Clause 8:
Operation of the service management system

8.2 Service portfolio

8.2.4 Service catalog management

Addressed process requirement(s):

- Create and maintain one or more service catalogs with information related to customers, users, interested parties, and service dependencies.

ManageEngine product that can help in implementing this process:

ServiceDesk Plus

- The customizable service catalog module will help you create and publish your organization's services.
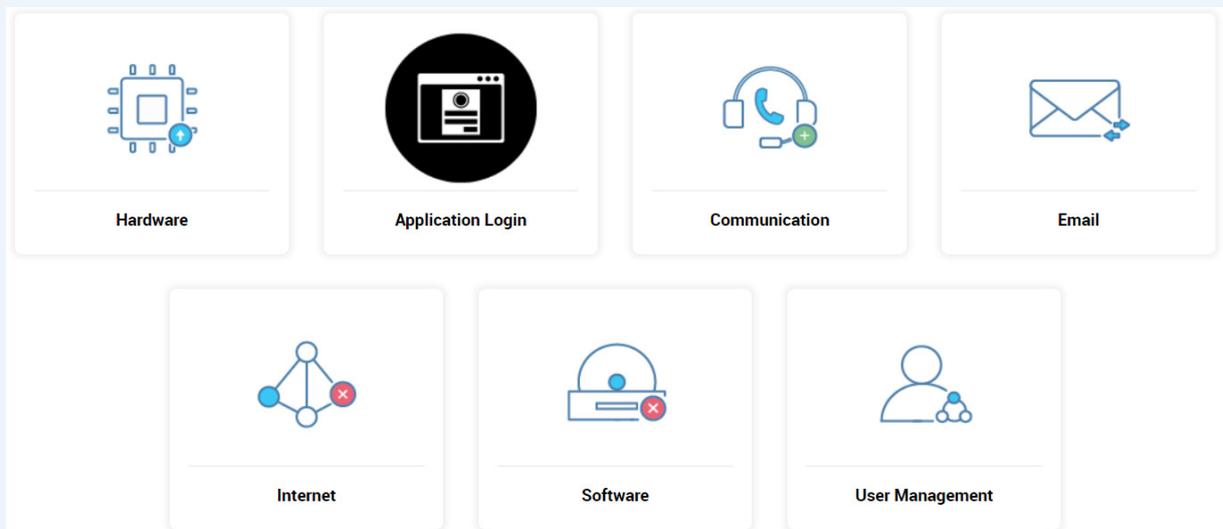
Service categories in the service catalog

- The configuration management database (CMDB) module organizes all the services in one place as configuration items and helps you maintain the details related to the services, including interested parties and service dependencies.
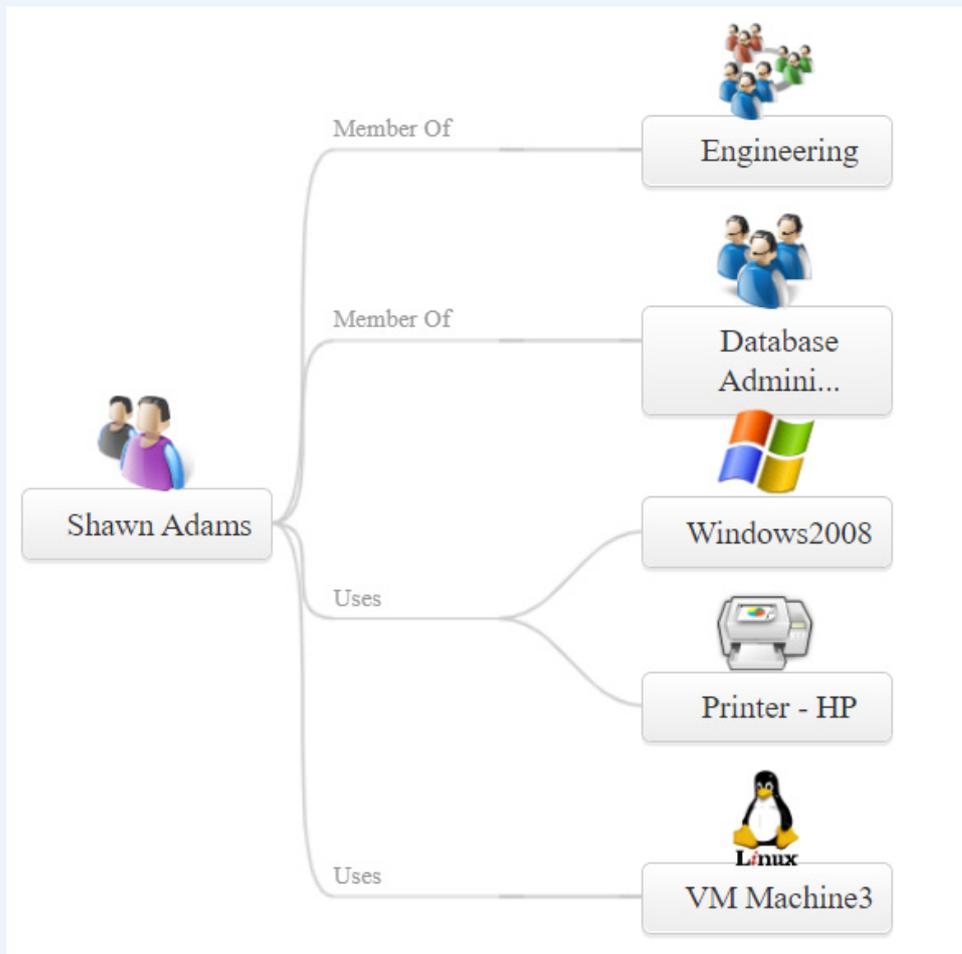
Dependencies and user relationships

8.2.5 Asset management

Addressed process requirement(s):

- Ensure assets used to deliver the services are managed to meet the service requirements.

ManageEngine product that can help in implementing this process:
ServiceDesk Plus

- The asset management module is packed with thoughtful features, including multiple methods of scanning assets, agent-based and agent-less methods, barcode scans, network scans, and more to help you manage all the assets and their related inventory used to deliver the services. It also seamlessly integrates with other ITSM processes including incident, problem, and change management to help you track all tickets associated to the assets.

Asset management dashboard

Inventory details of the asset

8.2.6 Configuration management

Addressed process requirement(s):

- Services shall be classified as configuration items (CIs) configuration information for each CI will include a unique identification, type, description, relationship, and status.

ManageEngine product that can help in implementing this process:

ServiceDesk Plus

- Services are classified as CIs in the CMDB module. All CI types are configurable to maintain specific attributes like name, type, description, status, etc. and help to build visual relationships between CIs.

Information related to a particular CI in the CMDB

8.3 Relationship and agreement

8.3.2 Business relationship management

Addressed process requirement(s):

- Document customers, users, and other interested parties related to the services.

- Review the performance and satisfaction with the services based on samples at planned intervals.

- Service complaints shall be recorded and managed to closure. If not resolved,

ManageEngine product that can help in implementing these processes:

ServiceDesk Plus

- Visual relationships in the CMDB module document the details related to the services.
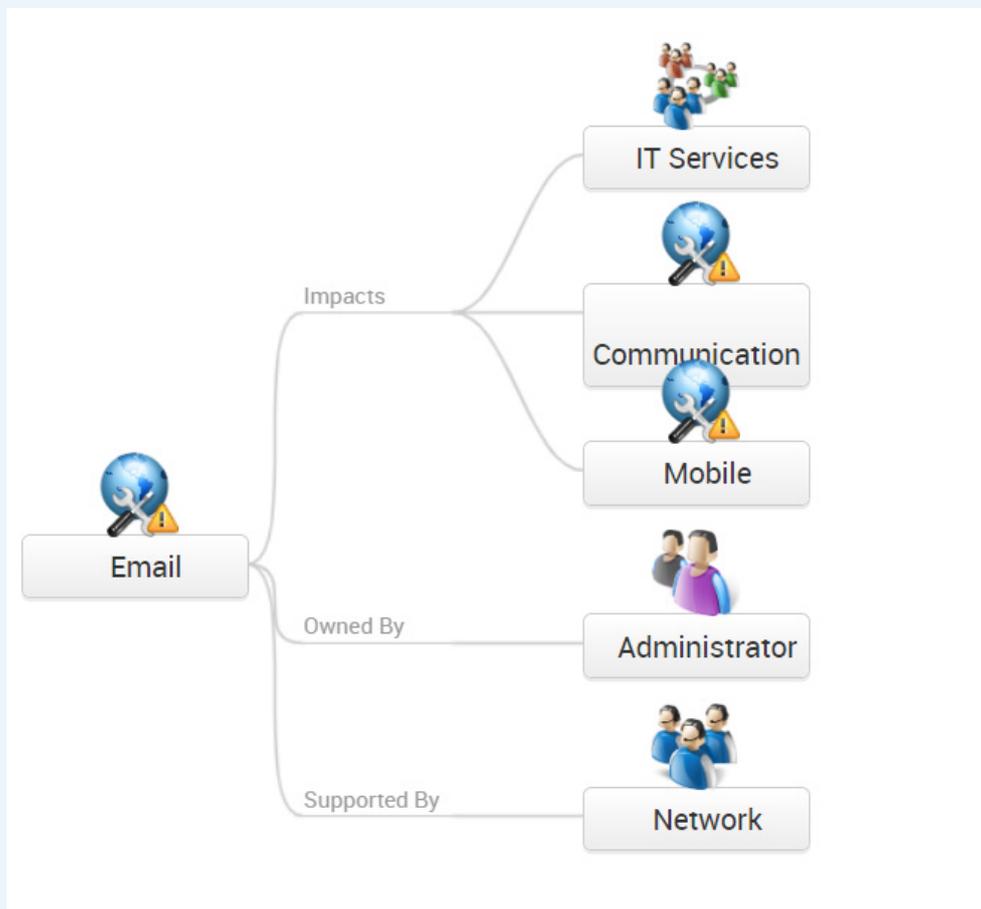
Relationships with users mapped in the CMDB

- Satisfaction with services can effectively be measured using the survey module at planned intervals. Reporting is extended to identify opportunities for improvement and measure the performance trends.

Periodic survey for performance review

- A separate incident template with customized forms and fields can be defined to log service complaints, which can follow its process and if not resolved, escalated.

Incident and service complaint templates

8.3.3 Service level management

Addressed process requirement(s):

- Agree on the services to be delivered, and establish one or more service level agreements (SLAs), including service-level targets, workload limits, and exceptions.
- Monitor, review, and report on service level targets and workloads, and identify opportunities for improvement if SLA(s) are not met.

ManageEngine product(s) that can help in implementing these processes:

ServiceDesk Plus and Analytics Plus

- The services agreed to be delivered can be exhibited and maintained with the help of the service catalog module. The incident and service request SLA(s) for response/resolution/fulfillment corresponding to these services can be assigned
  and their effectiveness can be monitored, reviewed, and reported on by

Incident SLA: Response, resolution, and escalation

When a new Service Request arrives :

Service Requests should be responded within	: 00 Days	0 ▾ Hours 0 ▾ Minutes
Service Requests should be fulfilled within	: 00 Days	0 ▾ Hours 0 ▾ Minutes

☐ Should be fulfilled/responded irrespective of operational hours.
    ☐ Should be fulfilled/responded irrespective of Holidays.
    ☐ Should be fulfilled/responded irrespective of Weekends.

If the response time is about to be elapsed/elapsed then escalate:

☑ Enable Level 1 Escalation

Escalate to [   ] Choose

    ○ Escalate Before ◉ Escalate After 00 Days 0 ▾ Hours 0 ▾ Minutes

Actions

If the fulfillment time is about to be elapsed/elapsed then escalate:

☑ Enable Level 1 Escalation

Escalate to [   ] Choose

    ○ Escalate Before ◉ Escalate After 00 Days 0 ▾ Hours 0 ▾ Minutes

Actions

☐ Enable Level 2 Escalation
☐ Enable Level 3 Escalation
☐ Enable Level 4 Escalation

Service request SLA: Response and fulfillment
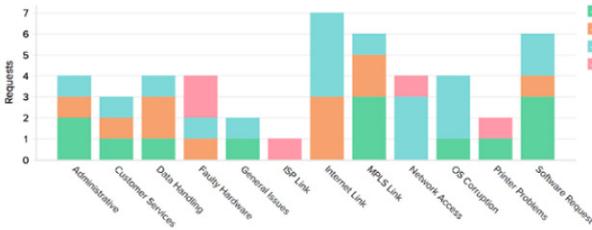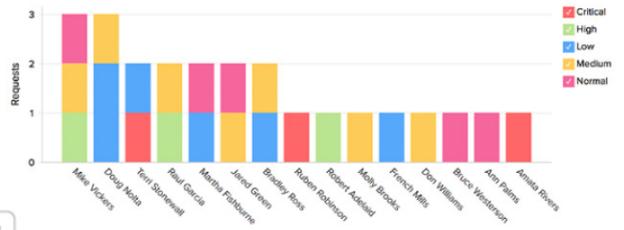
Reporting on SLA targets (incident and service request)

OpManager Plus and Applications Manager

- OpManager Plus and Applications Manager together can monitor all the service

  components like network devices, servers, virtualization, applications, data-
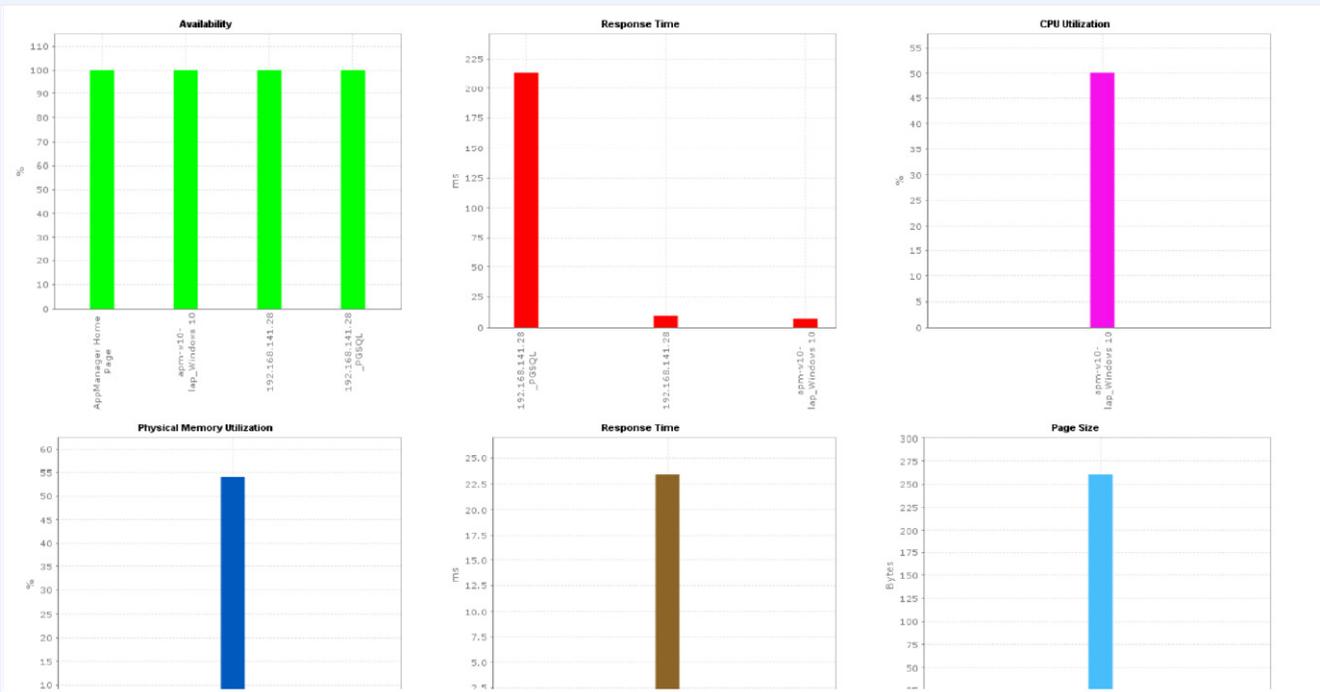
Availability and performance report of a service

Device Name	Min	Max	Avg	
Opm-scale2	99	100		99
mickey-w2k8r2-dc-1	99	99		99
opman-hyperv.opmanhv.com	97	99		97
opm-esx6-1.csez.zohocorpin.com	67	77		76
172.21.10.183	64	64		64
Opm-k12r2-vc	54	54		54
opm-w12r2	17	52		42
mickey-w2k8r2-chinese	42	44		42
opm-w2k8r2	5	99		42
opmanhv-node1	32	34		33
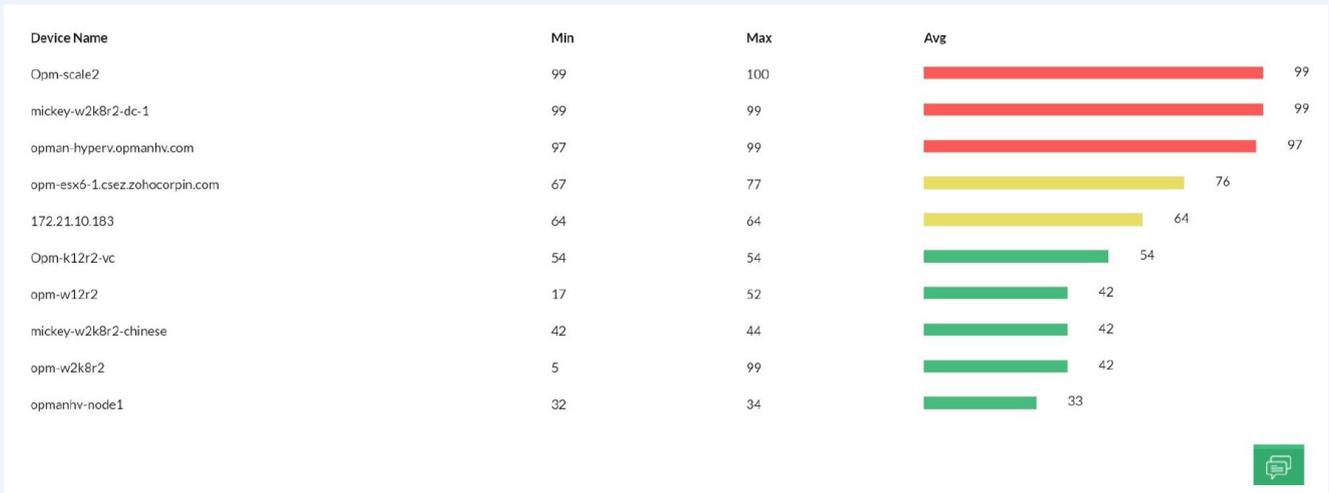
Memory utilization of top 10 devices

SLA	Server SLA	Events	Settings

New SLA   Intro to Manager Console

Business Applications with least Availability for Today

Applications Ma..   Conditional app..

Control Applica..

● Down ● Up

Period

Today ▼

Custom Time Period

Start Time

End Time

Show Report

SLA Statistics   Show all BA(s) | Show only SLA assigned BA(s)

Name	SLA Name ↑	Meets SLA	Total Downtime	Availability%	MTTR	MTBF	Events	
Control Applications	Severity	✔	0 Secs	100	0 Secs	14 Hrs 31 Mins 1 Secs	0	7
Conditional applications	Priority	✔	0 Secs	100	0 Secs	14 Hrs 31 Mins 0 Secs	0	7

SLA dashboard

8.3.4 Supplier management

Addressed process requirement(s):

- Develop, agree on, and maintain a documented agreement with the external and internal suppliers.
- Monitor the performance of the supplier including service targets at planned intervals.

ManageEngine product that can help in implementing these processes:

ServiceDesk Plus

- The agreements with external and internal suppliers along with sub-contract, service components, vendor, cost, expiration, etc. can be maintained and tracked using the Contracts module.

Contracts Module to maintain agreements

- Operational-level agreements (OLA's) agreed on with internal suppliers can be assigned to incidents and service requests and their performance can be measured against the agreement.

Operational level agreement(OLA)

ⓘ OLA time is applied individually to each selected group.

Group Name	OLA Time			Description
Network ✕	1 Hour ▼			
	Days	1 Hour	Minutes	
	0			
	1			
	2			
	3			
	4			
	5			

Save

OLA for Internal Suppliers

8.4 Supply and demand

8.4.1 Budgeting and accounting for services

Addressed process requirement(s):

- Costs shall be budgeted for effective financial control and decision making for services.
- Monitor and report on actual costs, review the financial forecasts, and manage costs at planned intervals.

ManageEngine product(s) that can help in implementing these process-ServiceDesk Plus and Analytics Plus

- Budget the recurring cost using the software License Agreements and Contracts modules.

Software license agreement

- Record and report on the actual costs and budget based on depreciation and spending. ServiceDesk Plus, when integrated with Analytics Plus, provides more visibility on the budget.

Asset financial and depreciation details
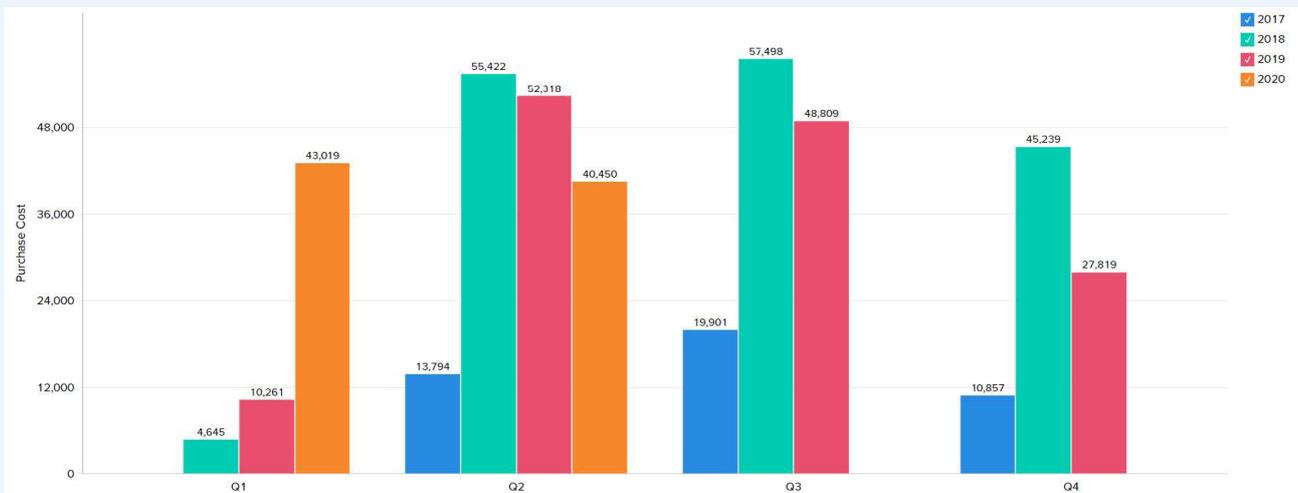
Year-over-year (YOY) comparison of IT spending based on purchase costs

Product Type: Access
Purchase Cost: 48,090.
Percentage: 11.2%
Click to see the data

11.2%

33.4%

27.5%

24.1%

IT spending

Total Purchase Cost($) Forecasted IT Spend

55,422 57,498 45,239 10,261 49,818 48,809 27,819 40,619 38,450 37,628 28,278 25,507 24,031 44,625

Q2 2018 Q3 2018 Q4 2018 Q1 2019 Q2 2019 Q3 2019 Q4 2019 Q1 2020 Q2 2020 Q3 2020 Q4 2020 Q1 2021 Q2 2021 Q3 2021
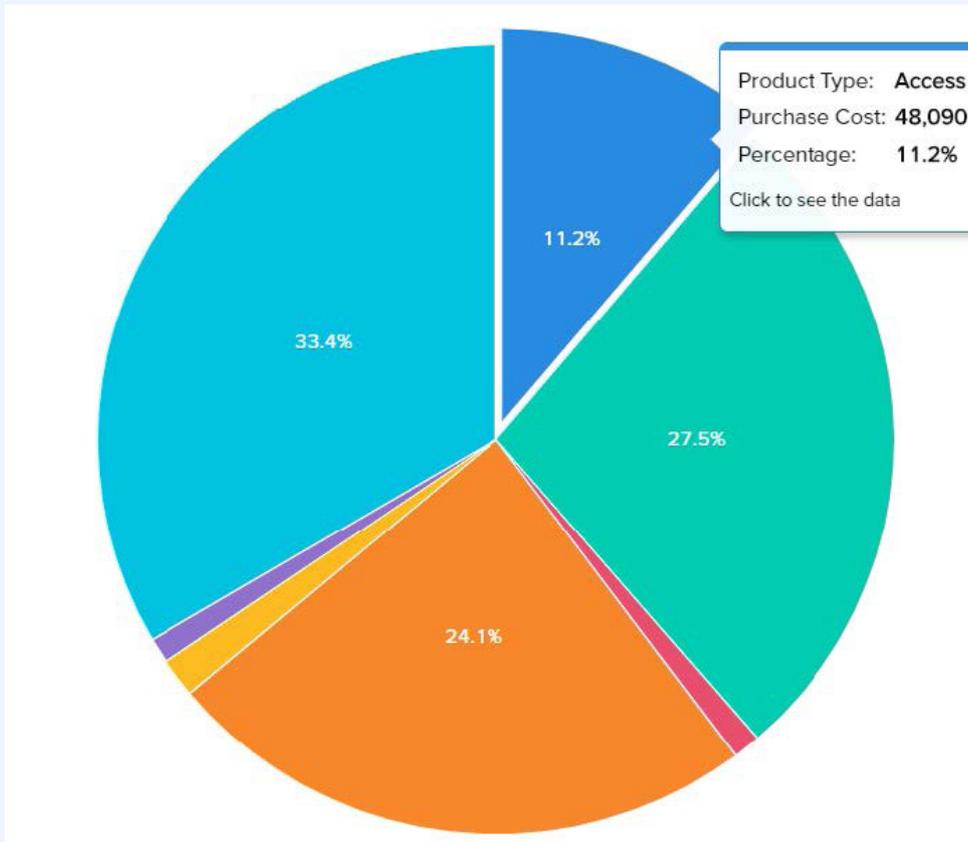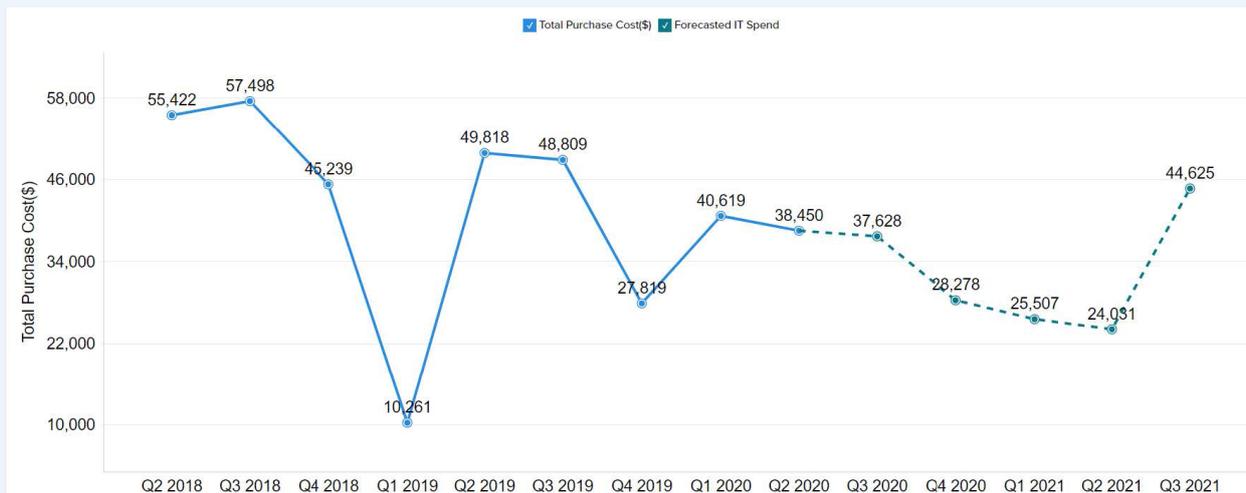
IT spending forecast

8.4.2 Demand management

Addressed process requirement(s):

- Monitor and report on the demand and consumption of services at planned intervals.

ManageEngine product(s) that can help in implementing these pro-

ServiceDesk Plus and Analytics Plus

- Analytics Plus, when integrated with ServiceDesk Plus, helps you determine the demand based on the consumption of services through service requests.

Top 10 frequently requested service

OpManager Plus and Applications Man–

- The reporting module forecasts the demand based on the consumption of service components.

Forecast report on disk utilization
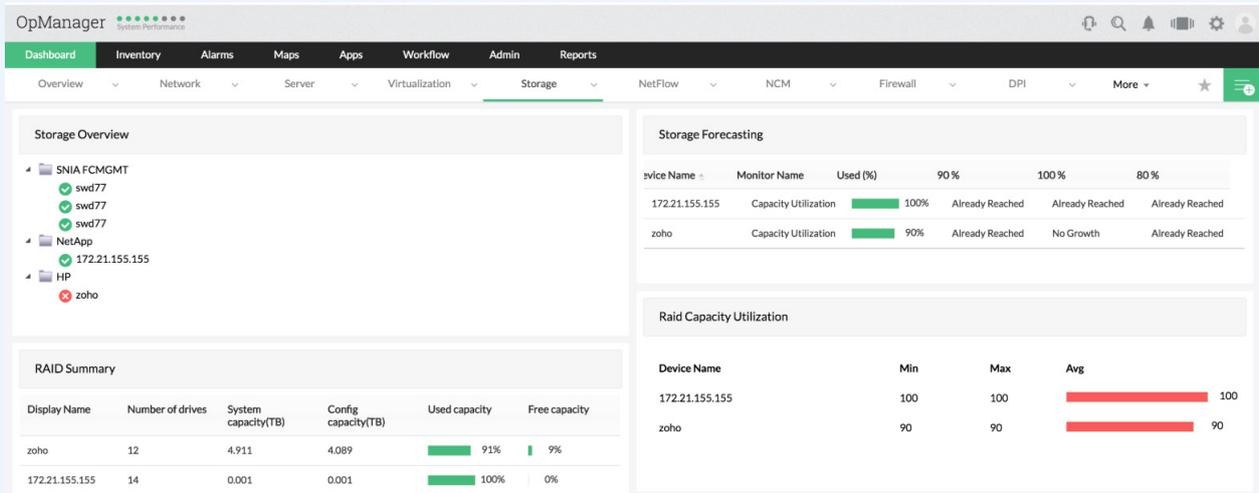
Storage capacity forecasting

8.4.3 Capacity management

Addressed process requirement(s):

- Monitor capacity utilized, and analyze capacity and performance data related to human, technical, informational, and financial resources to identify opportunities

ManageEngine product(s) that can help in implementing this process:
ServiceDesk Plus and Analytics Plus

- Analyze capacity and performance related to IT human resources based on handled incidents, service requests, problems, changes, releases, projects, etc.
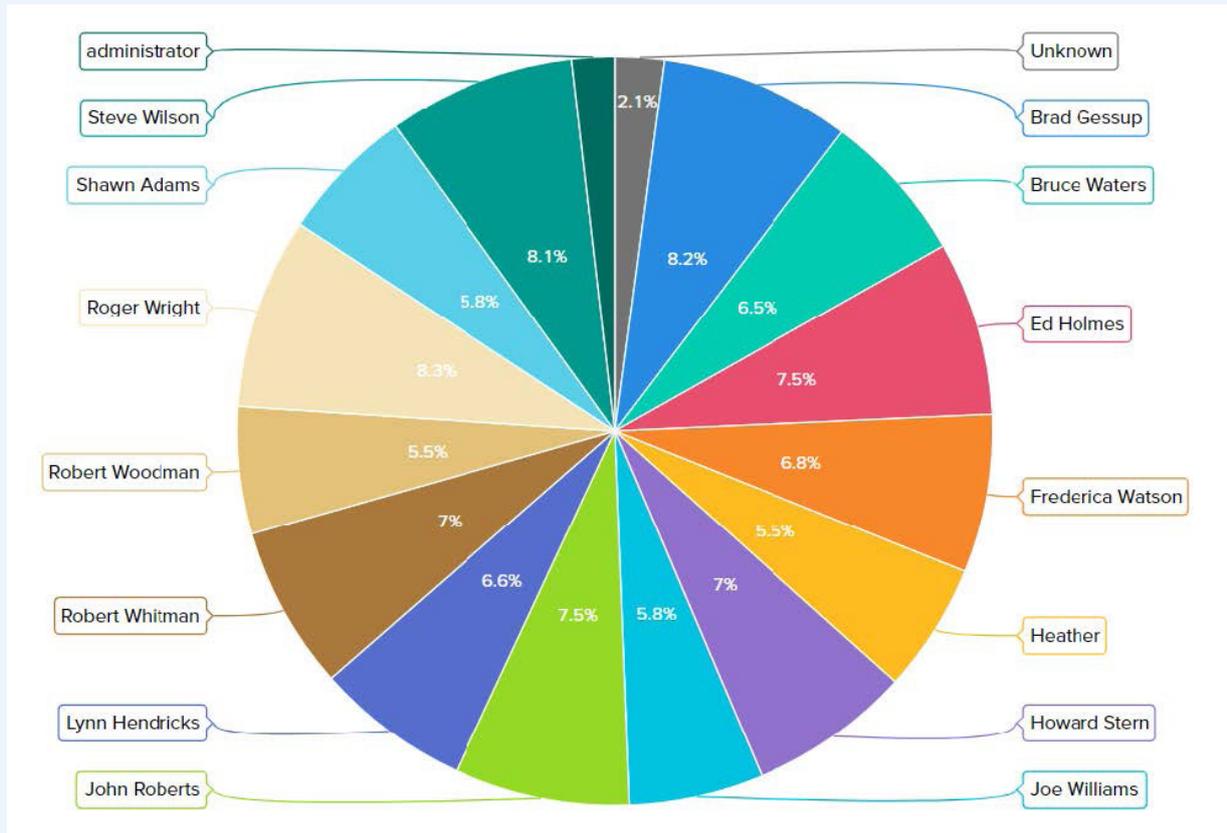
Technician load: Open requests
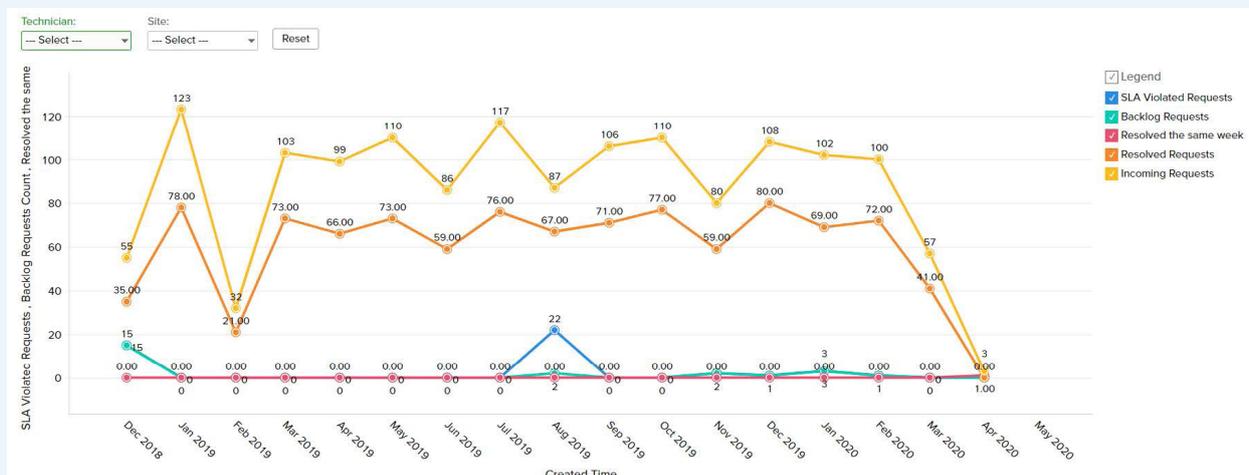
Incoming, resolved, backlogged, and same-week

OpManager Plus and Applications Man-

- Monitor and analyze capacity and performance of service components including servers, applications, network, bandwidth, and storage.
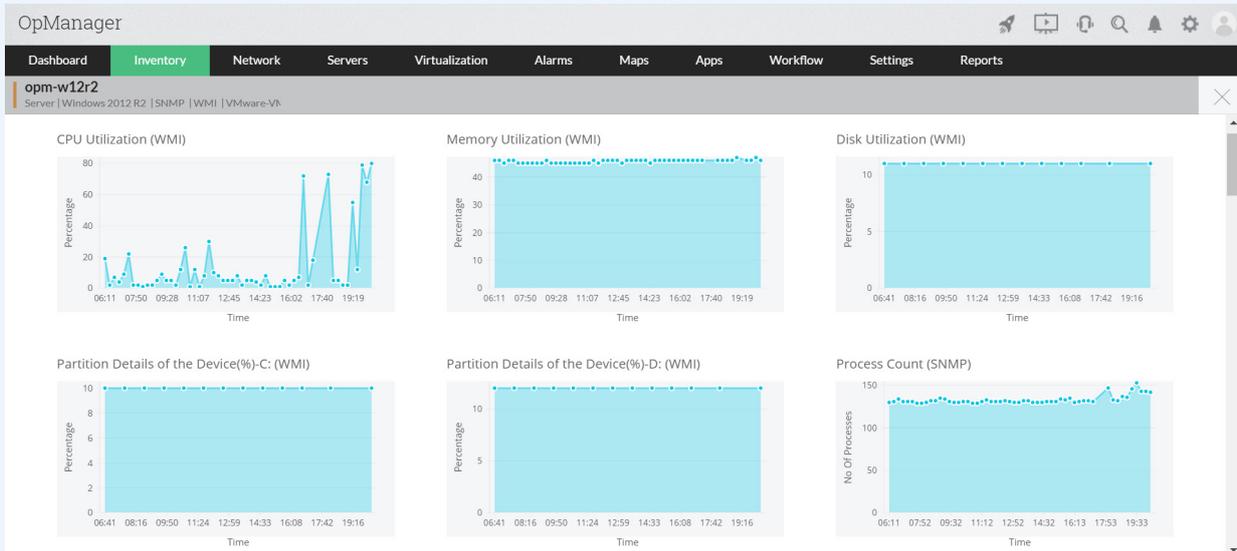
Server performance monitoring

Report on over-sized servers

Analytics Plus

Advanced analytics on a wide variety of data points including capacity and performance can be be generated by integrating ManageEngine applications and any other applications that use local and cloud databases like MS SQL, Oracle, MySQL, Azure SQL, etc. with Analytics Plus.

Analytics Plus possible integrations
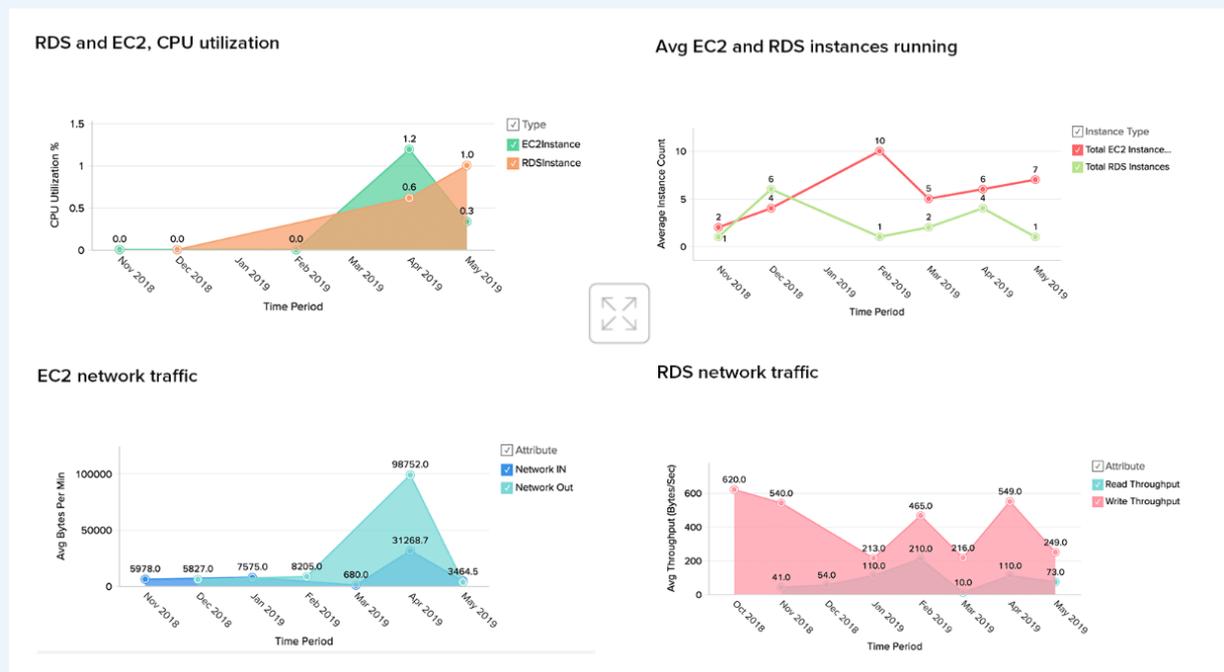
Applications Manager integration: AWS performance report

8.5 Service design, build, and transition

8.5.1 Change management

Addressed process requirement(s):

- Requests for changes, including proposals to add, remove, or transfer services, shall be recorded and classified.
- Assessing, approving, scheduling, and reviewing of new or changed services shall be managed through the change management activities.
- Interested parties shall make decisions on the approval and on the priority.
- Approved changes shall be prepared, verified, and tested when possible.
- Communicate deployment dates and other deployment details for approved changes to interested parties.
- The activities to reverse or remedy an unsuccessful change shall be planned and tested when possible. Unsuccessful changes shall be investigated and agreed actions shall be taken.
- At planned intervals, request for change records shall be analyzed to detect trends and effectiveness and to identify opportunities for improvement.

ManageEngine products that can help in implementing these processes:

ServiceDesk Plus

- **The Change management module** allows users to submit requests for changes with different workflows for different types of changes like standard, normal, and emergency.
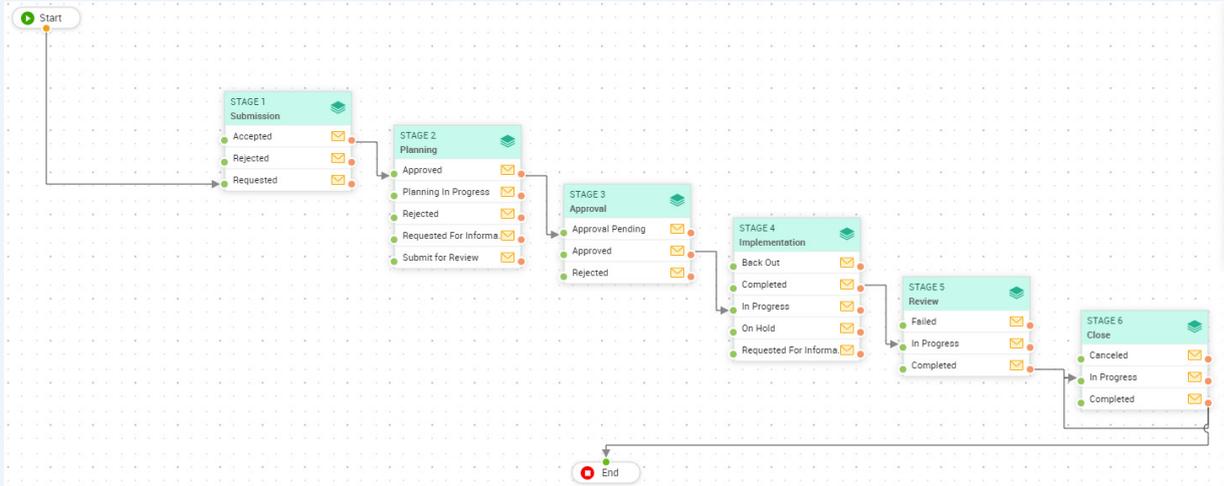
Configurable change workflow

Multiple change workflows

- The template/workflow used to submit the request is configurable to have its fields, stages, and statuses. By default, the request can go through various stages like submission, planning, approval, implementation, review, and closure with different statuses allowing you to track the progress of the request. The workflow also lets you to return to the previous stages, as needed.

Configurable RFC template

Change planning

- Approval can involve both a change manager and the Change Advisory Board's (CAB's) approval along with the third party's approval. Once the change is approved,

Change approval

- Unsuccessful change requests will follow the configured workflow, like returning to previous stages or closing the change record.

Change review

Analytics Plus

- Analytics Plus, when integrated with ServiceDesk Plus, provides out-of-the box reports on change management, which helps in analyzing the trend's effectiveness.
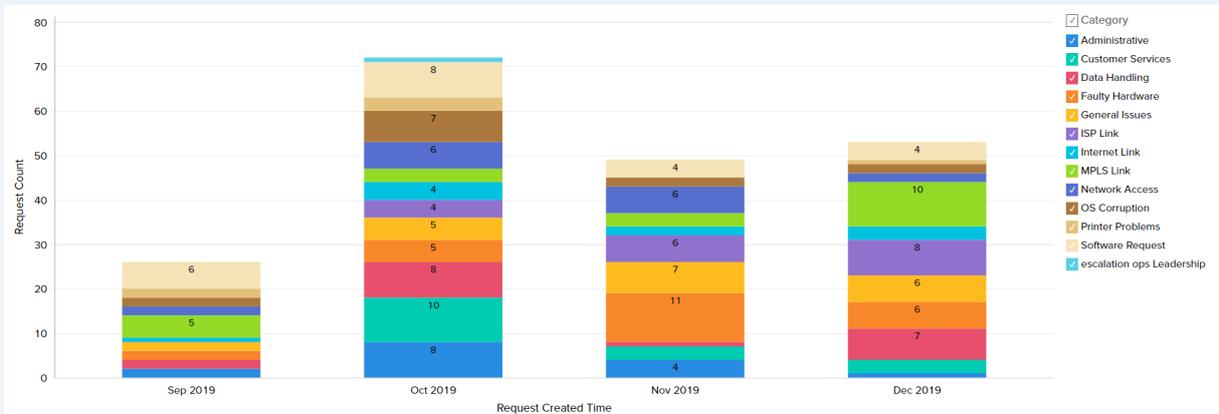
Trend requests for analyzing changes
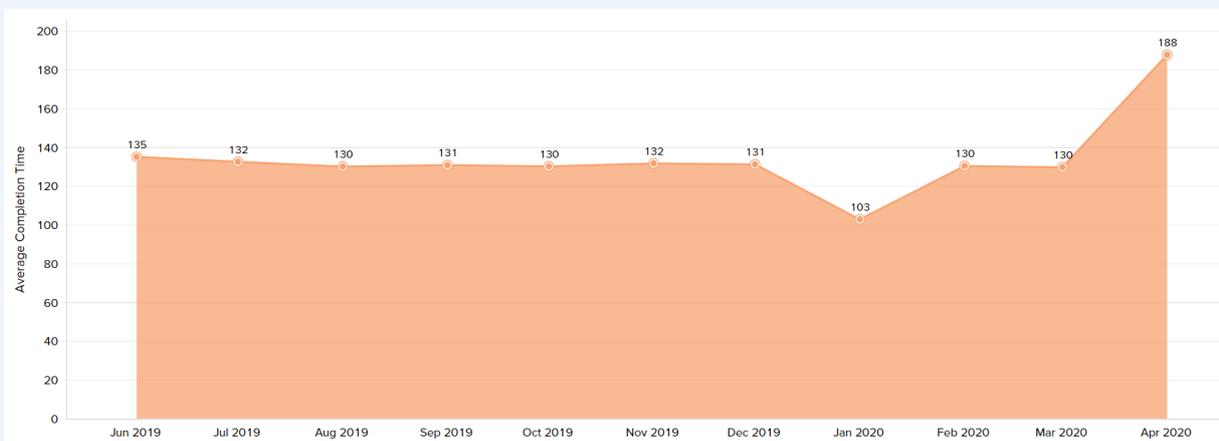
Average change completion time (in days)

Addressed process requirement(s):

- New services or changes to services with potential to have major impact, removal of a service, and transfer of an existing service from/to organization/customer/third party shall follow service design and transition.

- Planning shall contain reference to authorities and responsibilities, activities with timescales, resources information, dependencies, testing, acceptance criteria, affected CI's, and date of effect.

- Design shall include authorities and responsibilities, resources information, required training, SLA/contract changes, impact on other services, and updates to the service catalog.

- Release and deployment management shall be used to deploy the approved new or changed services into the live environment.

- After this, the interested parties shall be communicated with achievements against expected outcomes.

ManageEngine product(s) that can help in implementing these processes:

ServiceDesk Plus

- The change management module helps you create a separate template/workflow to handle major changes that are under the scope of new or changed services.

- The template and the change request allows you to record and maintain all the required details of the planning and design phases including authorities, affected CI's, activities, resources information, impact, etc.

- Once the change request is approved, the deployment can either go through the implementation stage of a change request which interfaces with tasks, projects and release modules.

Implementation: Projects and tasks

Release management

- The achievements against the expected outcomes can be communicated using the notification from the change request itself.

Addressed process requirement(s):

- The types of release, including emergency release, their frequency, and how they are to be managed, shall be defined.

- The deployment of new or changed services and service components into the live environment shall be planned and coordinated with change management and
  include references to the related requests for change, known errors or problems, the deployment dates, deliverables, and methods of deployment.

- The release shall be approved before deployment and verified against documented acceptance criteria.

- Before deployment of a release into the live environment, a baseline of the affected CIs shall be taken.

- The success or failure of releases shall be monitored and analyzed, including

ManageEngine products that can help in implementing these processes:

ServiceDesk Plus

- The release module available in the cloud version supports different templates/ workflows for different types of releases including emergency releases.

- The release request by default can go through different stages like submission, planning, development, testing, user acceptance testing (UAT), deployment, training, review, and closure. Each stage will mention the status to help track the progress. New stages/statuses can be configured as required. The workflow
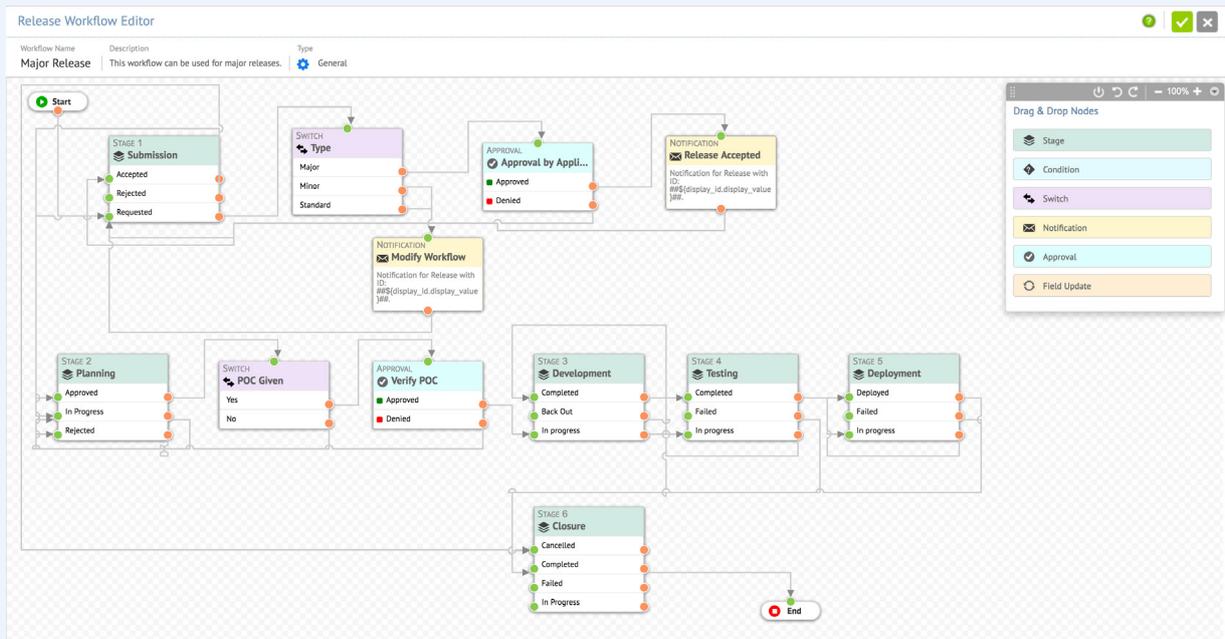
Release workflow
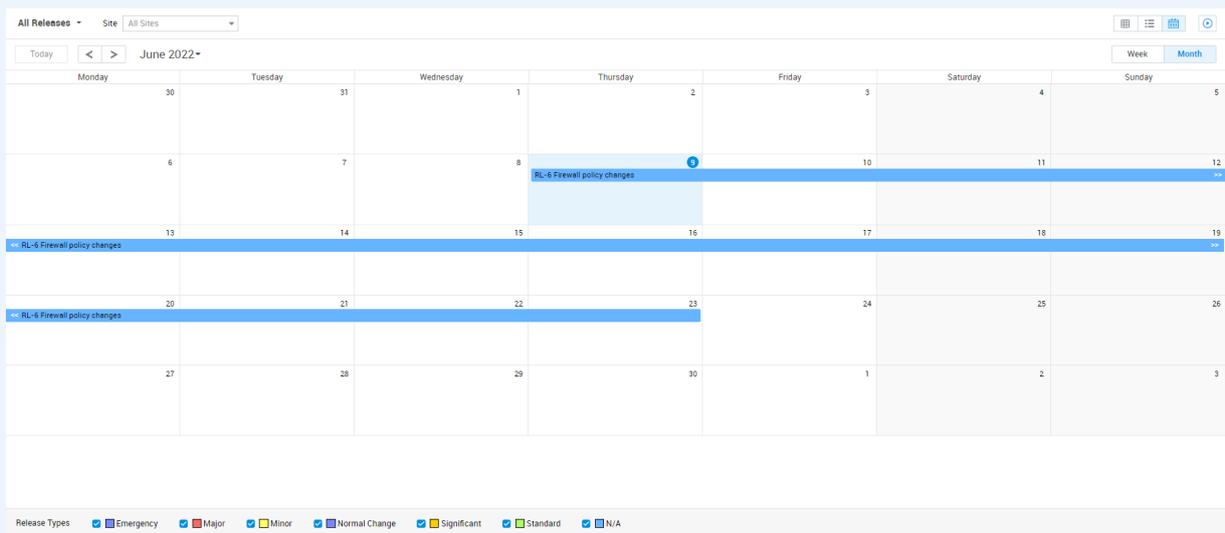
Release calendar

- The release request will contain reference to change, problem, known errors, and other deliverables.

New release template: Change association

- Reporting module helps you to analyze the effectiveness of the release to identify opportunities for improvement.
- For the on-premises version, the same can be handled using a combination of the change and project modules.

Project management: Change association

OpManager Plus

- OpManager's Network Configuration Manager component can take a back-up of the network device configurations as a baseline before deployment of a release, compare the changes, and rollback changes as required.
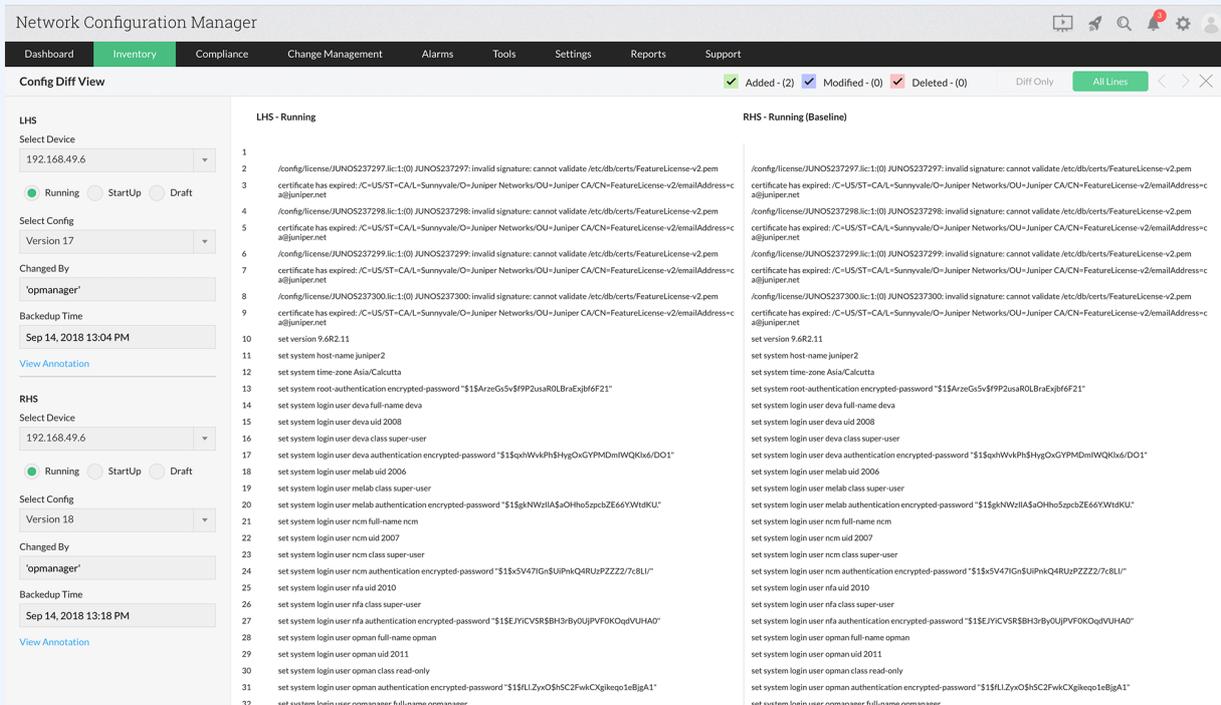
Compare configurations

AD360

- The Recovery Manager Plus component of AD360 can backup AD objects, Exchange mailboxes, OneDrive for Business, and SharePoint Online sites as baselines, and offers simple and granular restoration options.
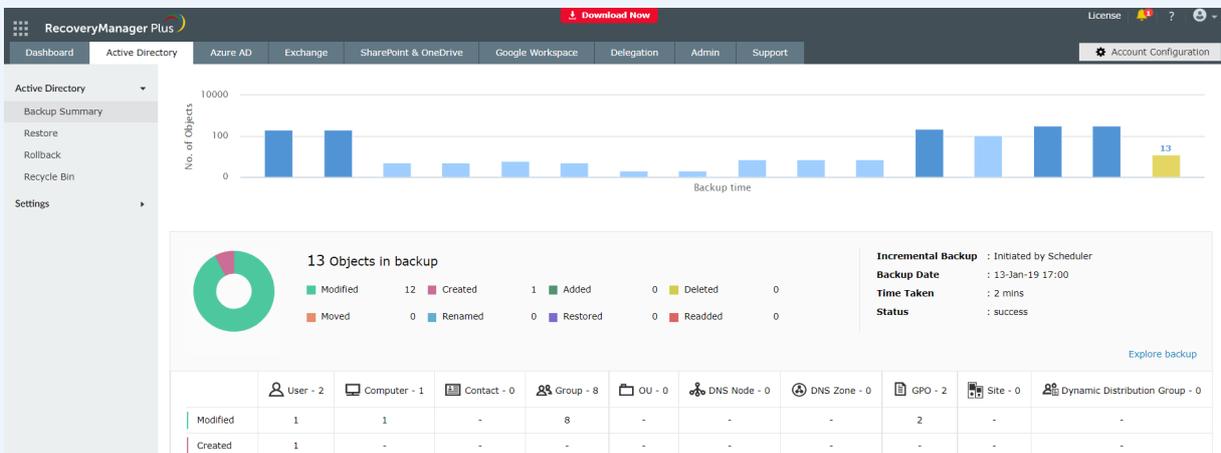
AD, Exchange, Sharepoint, and OneDrive backup and restore

Endpoint Central

- The OS Deployment module of Endpoint Central can take an image of the OS before the deployment of a release. Endpoint Central also helps you to deploy the releases pertaining to software deployment, patch management, computer configurations, etc.
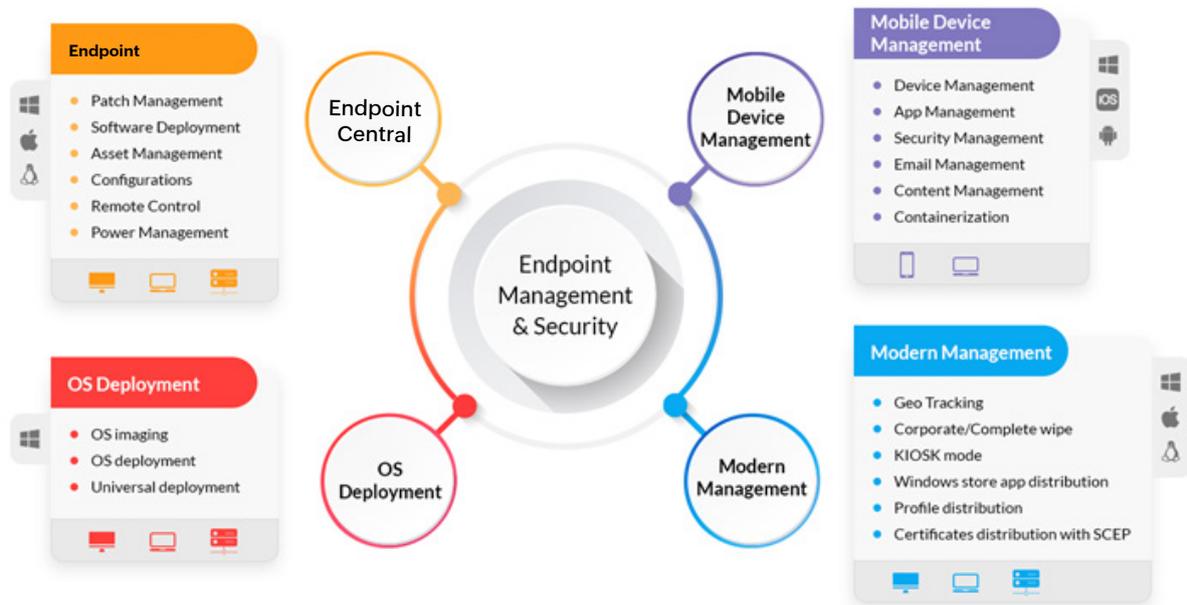
Endpoint Central for endpoint releases

8.6 Resolution and fulfillment

8.6.1 Incident management

Addressed process requirement(s):

- Incidents shall be recorded, classified, prioritized based on impact and urgency, escalated if needed, updated with actions, resolved, and closed.

- Major incidents shall be classified and managed through a documented procedure. The major incidents shall be reported to top management and reviewed post resolution for opportunities for improvement.

ManageEngine product that can help in implementing these processes:

ServiceDesk Plus and Analytics Plus

- The Incident management module helps you to record incidents using customizable templates, prioritize based on impact and urgency matrix, escalate based on response and resolution time, update actions taken, resolve, and close the incidents.
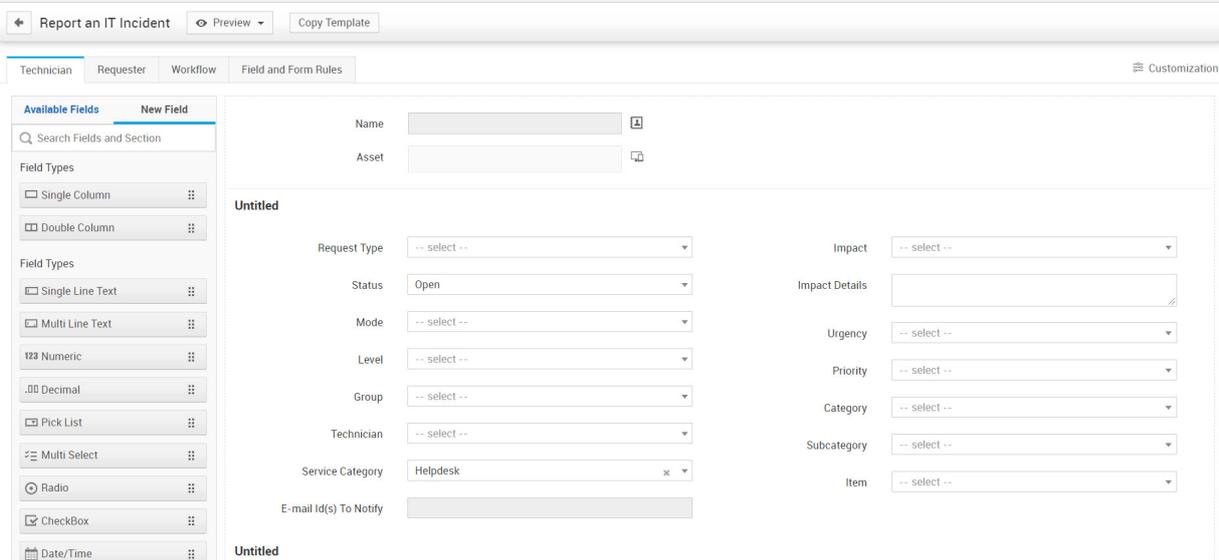
Customizable incident template

Any request matching the above rules should be responded within: `0` Days `0` ▾ Hours `30` ▾ Minutes | Response Time : 0 Hrs 30 Mins

Any request matching the above rules should be resolved within : `0` Days `2` ▾ Hours `0` ▾ Minutes | Resolution Time : 2 Hrs 0 Mins

☐ Should be resolved/responded irrespective of operational hours. : [Operational Hours per Day for this site : 9 Hrs 0 Mins]
　　☐ Should be resolved/responded irrespective of Holidays.
　　☐ Should be resolved/responded irrespective of Weekends.

If response time is elapsed then escalate:
☐ Enable Level 1 Escalation

If resolution time is elapsed then escalate:
☐ Enable Level 1 Escalation
☐ Enable Level 2 Escalation
☐ Enable Level 3 Escalation
☐ Enable Level 4 Escalation

Operational level agreement(OLA)

ⓘ OLA time is applied individually to each selected group.

Group Name	OLA Time	Description	
	--Select-- ▾		+

Response, resolution, and escalation

⚠ **#1 Unable to print**
　　by Heather Graham on Apr 7, 2020 04:30 PM | **DueBy : Apr 7, 2020 05:30 PM**

| Details | **Resolution** | Tasks | Checklist | Work Logs | Time Analysis | History |

Resolution　　**Solutions**　　**Tried Solutions**

B *I* U̲ a̶b̶c̶ F· 10 ▾ ■ ✎ X₂ X² ≡▾ ☰▾ ⊒ A̲ ❞ 🔗 🔗 ≟ ▦ 🖼 ☺ abc

Printer re-installed.

Attachments : 📎 Attach file

Update request status to `Resolved` ▾

Update actions, and resolve/close incidents

- If an incident is categorized as major incidents, it can be handled with different priority and processes, updating top management with the progress.

Business rules

- Analytics Plus integration helps you to analyze the records for opportunities for improvement.

Closed requests: Trend report
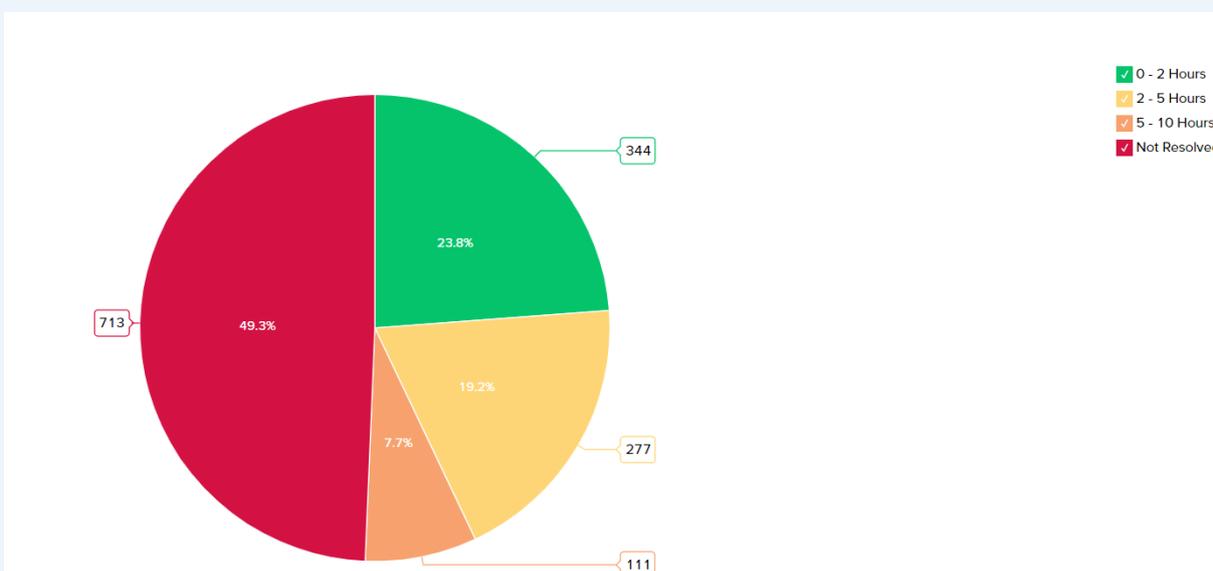
Average time to resolve

8.6.2 Service request management

Addressed process requirement(s):

- Service requests shall be recorded, classified, prioritized, fulfilled, updated with actions taken, and closed.

ManageEngine product that can help in implementing these processes:

ServiceDesk Plus

- The Service Catalog module helps you to create different service request templates under different categories, allowing users to choose the required service requests. Each template can have its own workflow process for approval,

  assignment, SLA, prioritization, and required fields to automate the flow of fulfillment.
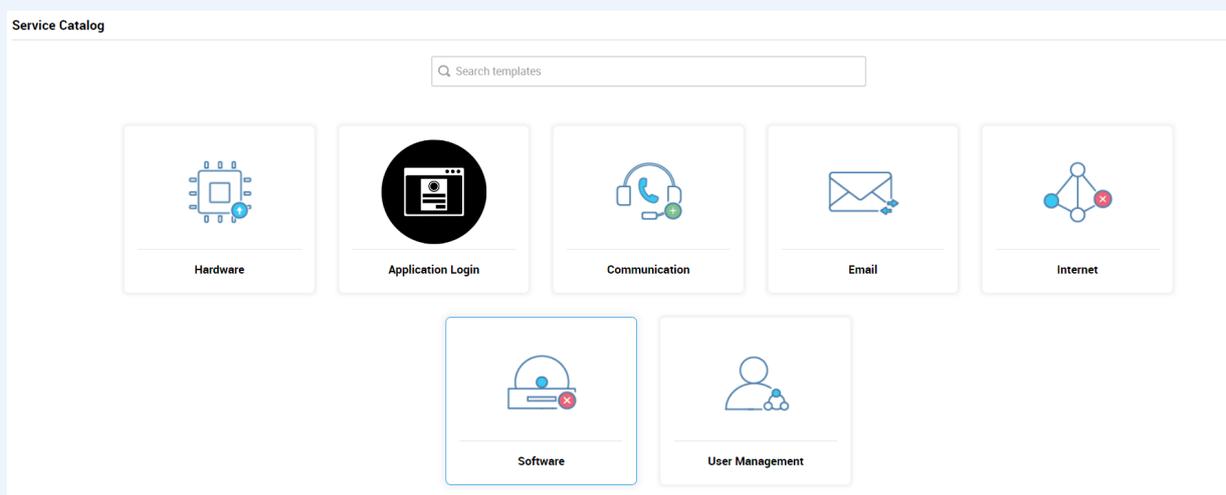
Service request templates
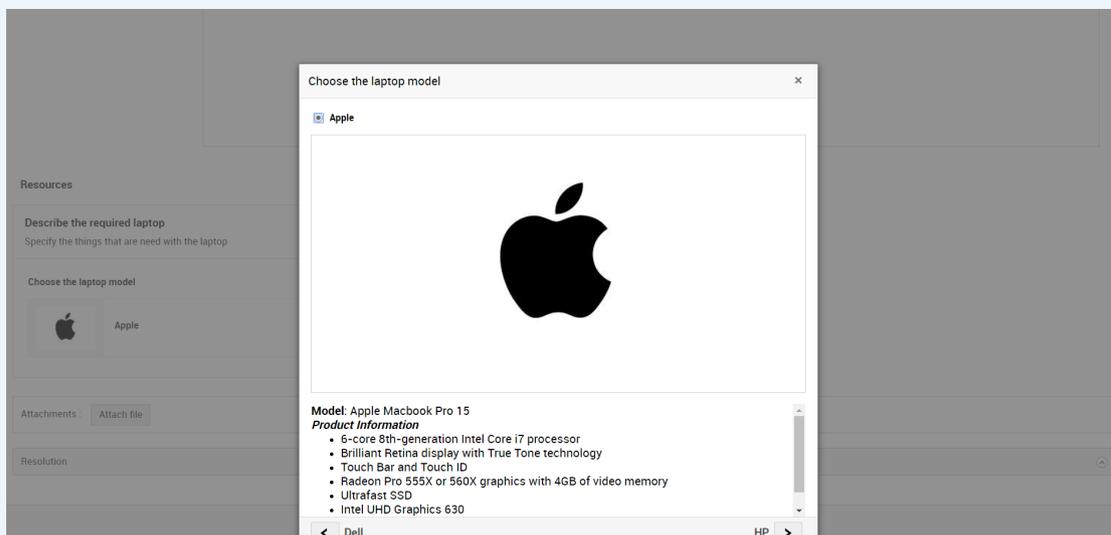
Choose a laptop to find details

Describe the required laptop

Specify the things that are need with the laptop

Choose the laptop model

Apple

☑ Cost Details

Enter additional information.

Service Cost $ 0.00

Capture provisioning costs

Add Resource   Associate Resource Sections   ❓ View Sample   ✕

Select existing questions   ⊕ ▾

Plain text
Check box
Radio
Drop down

Type and Press

Choose the deskt
Drop down

Choose the operating system
Drop down

Choose the additional hardware required
Check box

Choose the sofwares to be installed
Check box

Choose the laptop model
Drop down

Choose the account required for the new em...
Check box

Choose the devices required
Check box

What model of Computer do you want ?
Drop down

Desktop
Check box

Resource Sections

* Name   Description   Columns

.

No Questions added.

Save   Save and Add New   Cancel

Resource form for customization

Technician | Requester | Workflow | Field and Form Rules

Approval Details

Select Approver

Stage One $REPORTING_TO$ ✕

Stage Two $DEPT_HEADS$ ✕

Stage Three $REGIONAL_MANAGERS$ ✕

Stage Four CFO ✕

Stage Five CEO ✕   —

Approval Configurations

By default, when a request is approved, its approval status is updated as **Approved**. If one approver rejects it, the status remains in **Pending Approval**, until all approvers reject the request. Then, the approval status is updated to **Denied**.

☐ All approvers must approve the Service Request.

☐ Apply first approval action.

☐ Send approval notification automatically when a Service Request is raised.

☐ Assign technician only after Service Request approval.

Click here to configure outgoing mail server

Save   Cancel

SLA (1)

Add New SLA

High SR SLA   ⏱ 1 Day   ⚏ Template Users

Approval workflow and SLA

Field and form rules

8.6.3 Problem management

Addressed process requirement(s):

- Analyze data and trends on incidents to identify problems. Undertake root cause analysis and determine potential actions to prevent the occurrence or recurrence of incidents.

- Problems shall be recorded, classified, prioritized, escalated if needed, updated with actions, resolved if possible, and closed.

- Changes needed for problem resolution shall follow change management. Up-to-date information on known errors and problem resolutions shall be made available.

- The effectiveness of problem resolution shall be monitored, reviewed and reported on at planned intervals.

ManageEngine product that can help in implementing these processes:

ServiceDesk Plus and Analytics Plus

- The Reporting/Advanced Analytics module helps you to analyze data and trends on incidents to identify problems.
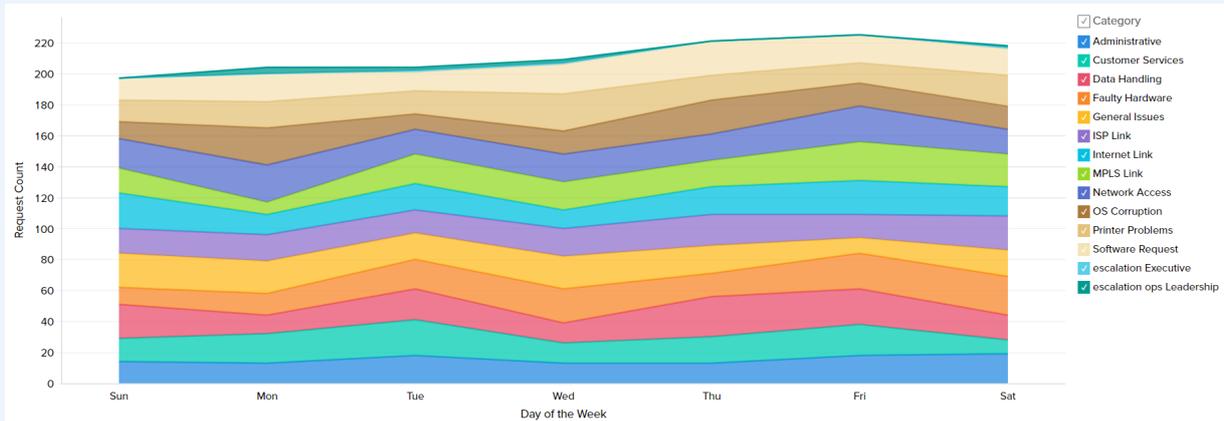
Weekly ticket inflow by category

- A problem record can be recorded, classified, prioritized, updated with actions, and resolved/closed. A problem record can be created directly after analyzing

Incident to problem association

- The problem record maintains the known errors, root cause, impact, workaround, and solution.

Problem analysis

- The problem record can be associated with a change record if a resolution for a problem is found and can follow the change management process.

Problem to change association

- The reporting module of ServiceDesk Plus and the Advanced Analytics modules help you monitor and review the effectiveness of a problem resolution.

ServiceDesk Plus: Bundled reporting

8.7 Service assurance

8.7.1 Service availability management

Addressed process requirement(s):

- Monitor service availability and compare the results with the targets.

- Investigate unplanned non-availability, and take necessary actions.

- The risks to service availability shall be assessed at planned intervals.

ManageEngine product that can help in implementing these processes:
OpManager Plus and Applications Manager

- Monitor the service availability based on all the dependent service components including network, servers, virtualization, storage, applications, databases, and websites, and compare them against the agreed target.
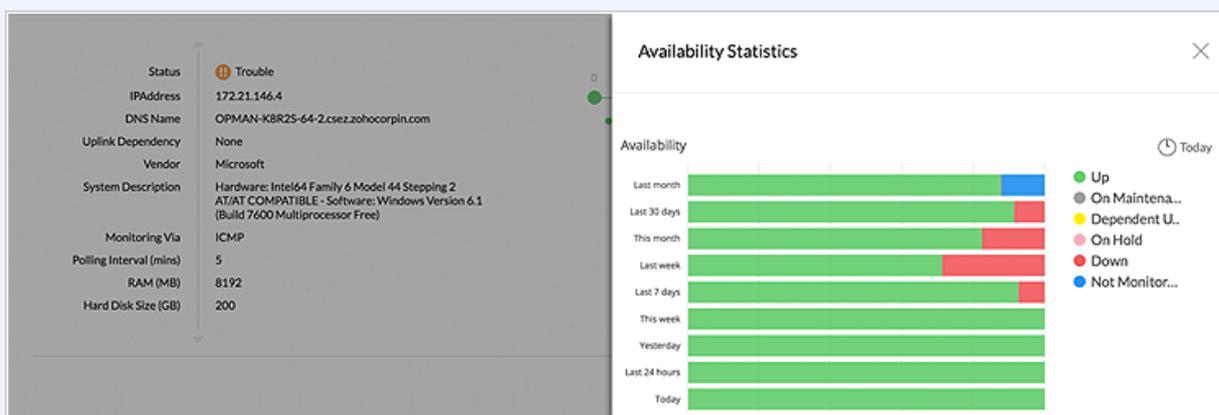
Availability statistics
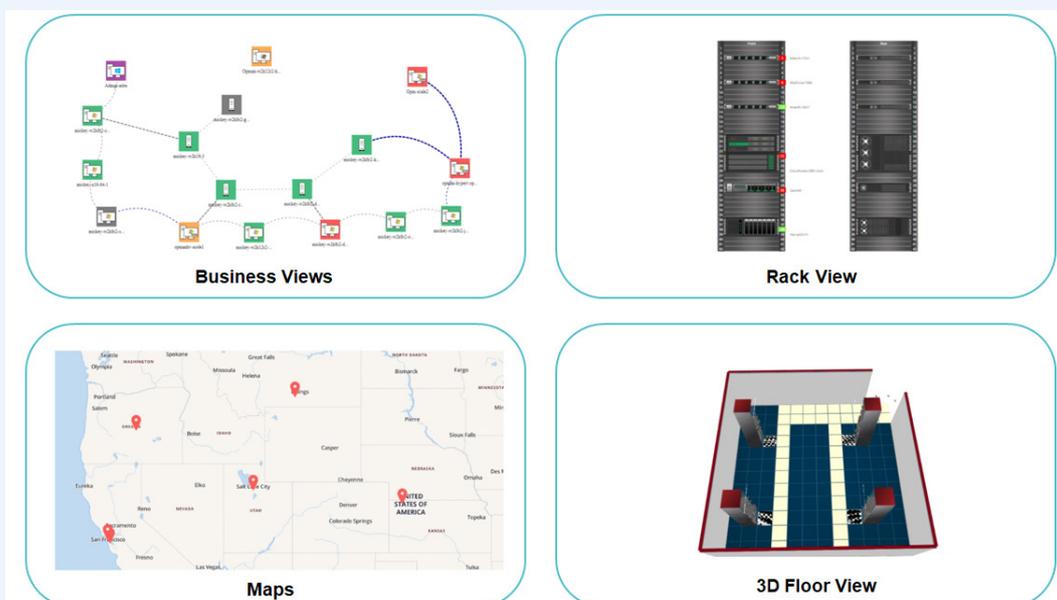
Availability representation
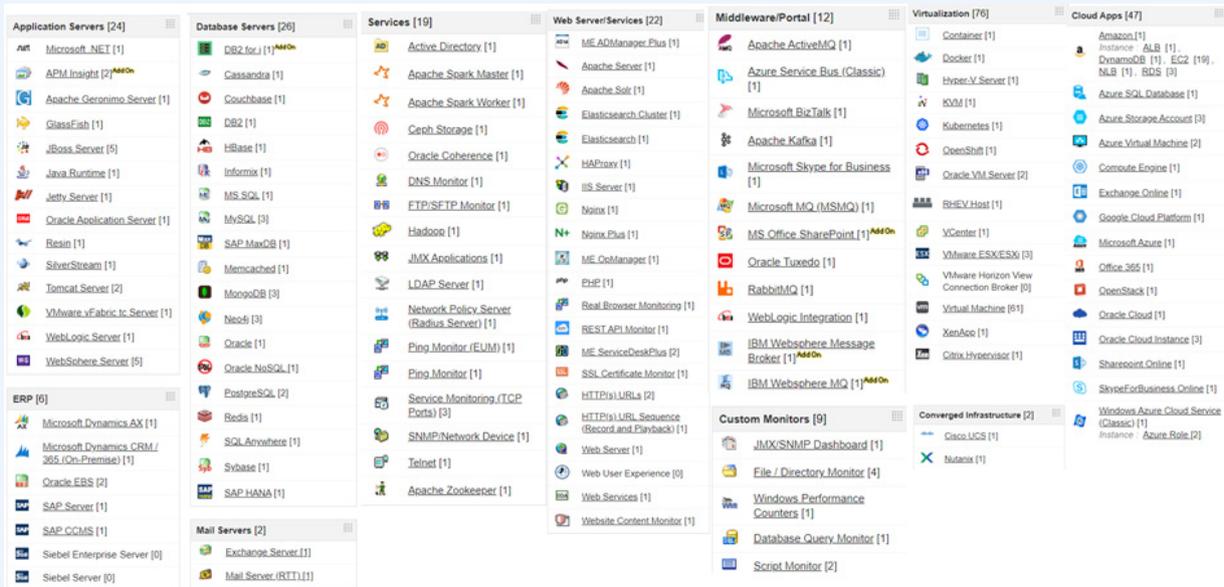
Applications monitoring
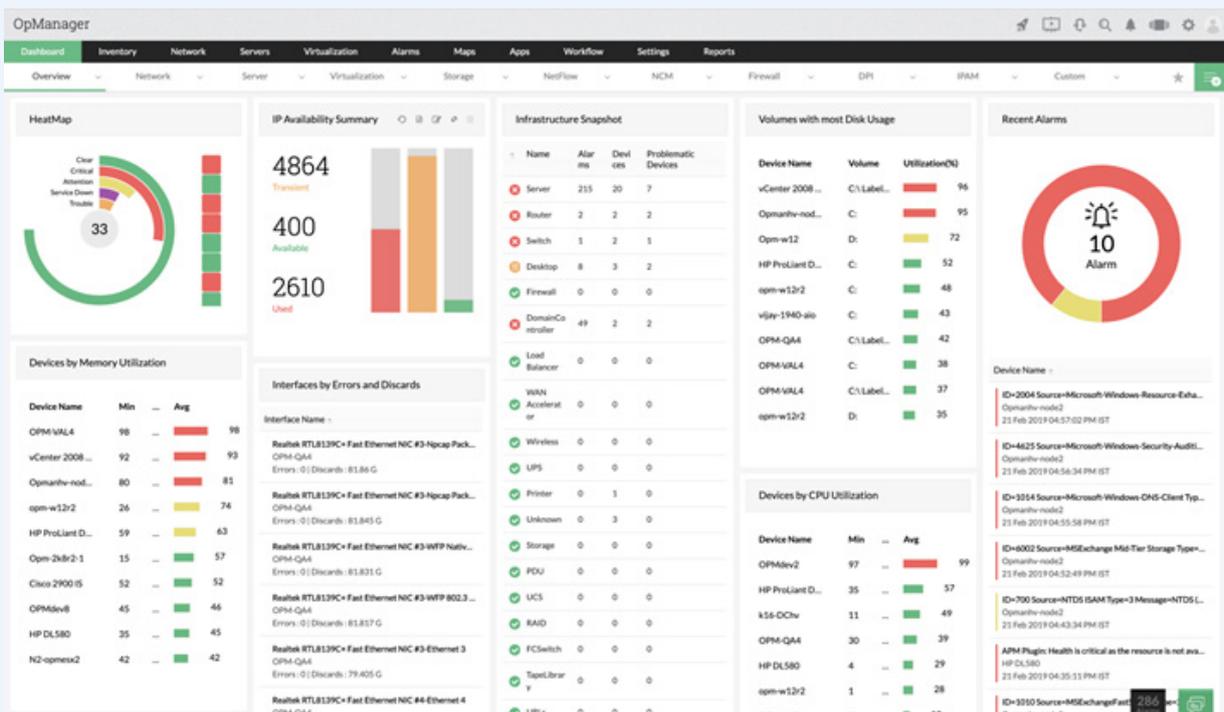
Monitoring dashboard

- Service components availability can be measured based on the performance metrics like response time, utilization, etc., and can be alerted on proactively to avoid unplanned downtime.
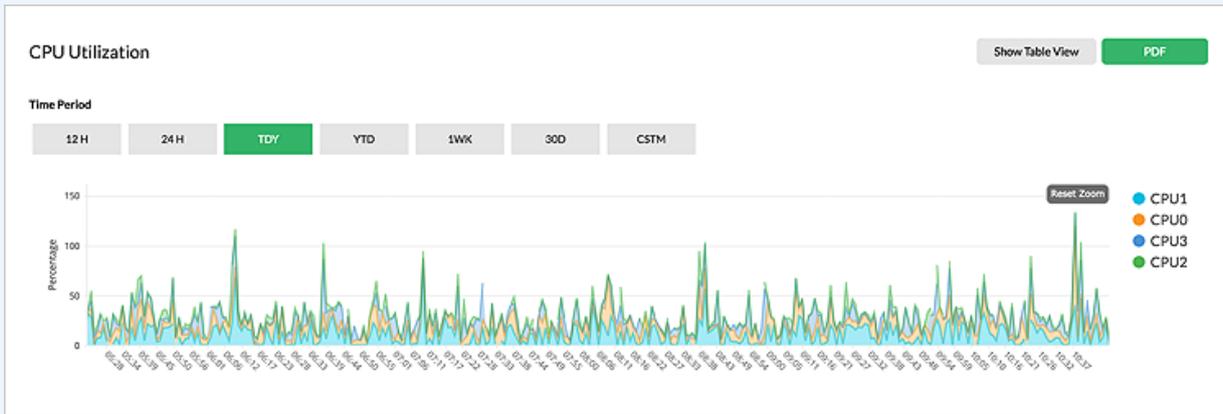
Performance monitoring: CPU
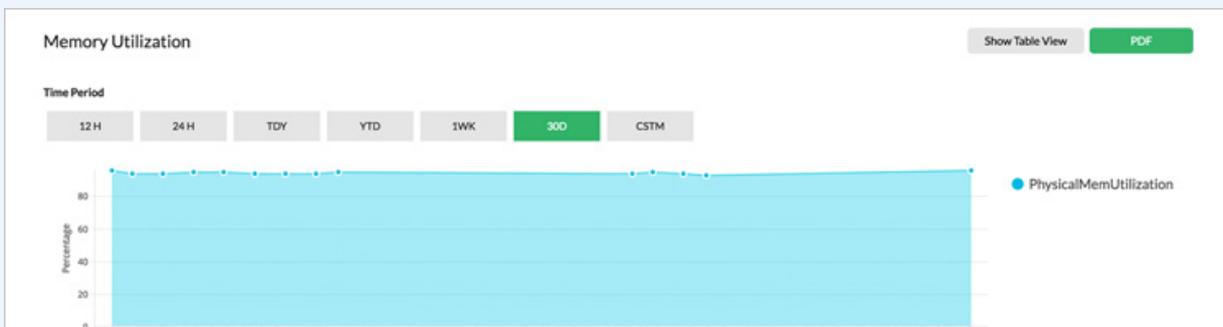
Performance monitoring: Memory

- Planned downtime can be marked to avoid false alarms. Unplanned downtime can be logged as incidents in ServiceDesk Plus and can be updated with investigated results/actions.

Downtime scheduler

Possible alarm notifications

- The monitored data is stored in the product databases for a configured period against which the risks to service availability can be generated considering various factors at planned intervals.

8.7.2 Service continuity management

Addressed process requirement(s):

- The service continuity plan(s) shall contain a reference to procedures for restoring services, steps to be followed in the event of a major loss of a service, and targets for service availability when continuity plans are involved.

- The continuity plan(s) shall be tested against the continuity requirements at periodic intervals. It shall be retested after major changes to the service environment. The results shall be recorded and reviewed. Necessary actions are to be taken when deficiencies are found.

- The risks to service continuity shall be assessed and documented at planned intervals.

- Document the cause, impact, and recovery when the continuity plan has been invoked.

ManageEngine products that can help in implementing these process-

ServiceDesk Plus

- The ServiceDesk Plus CMDB module helps you to create references to documents containing continuity plans for the respective services.
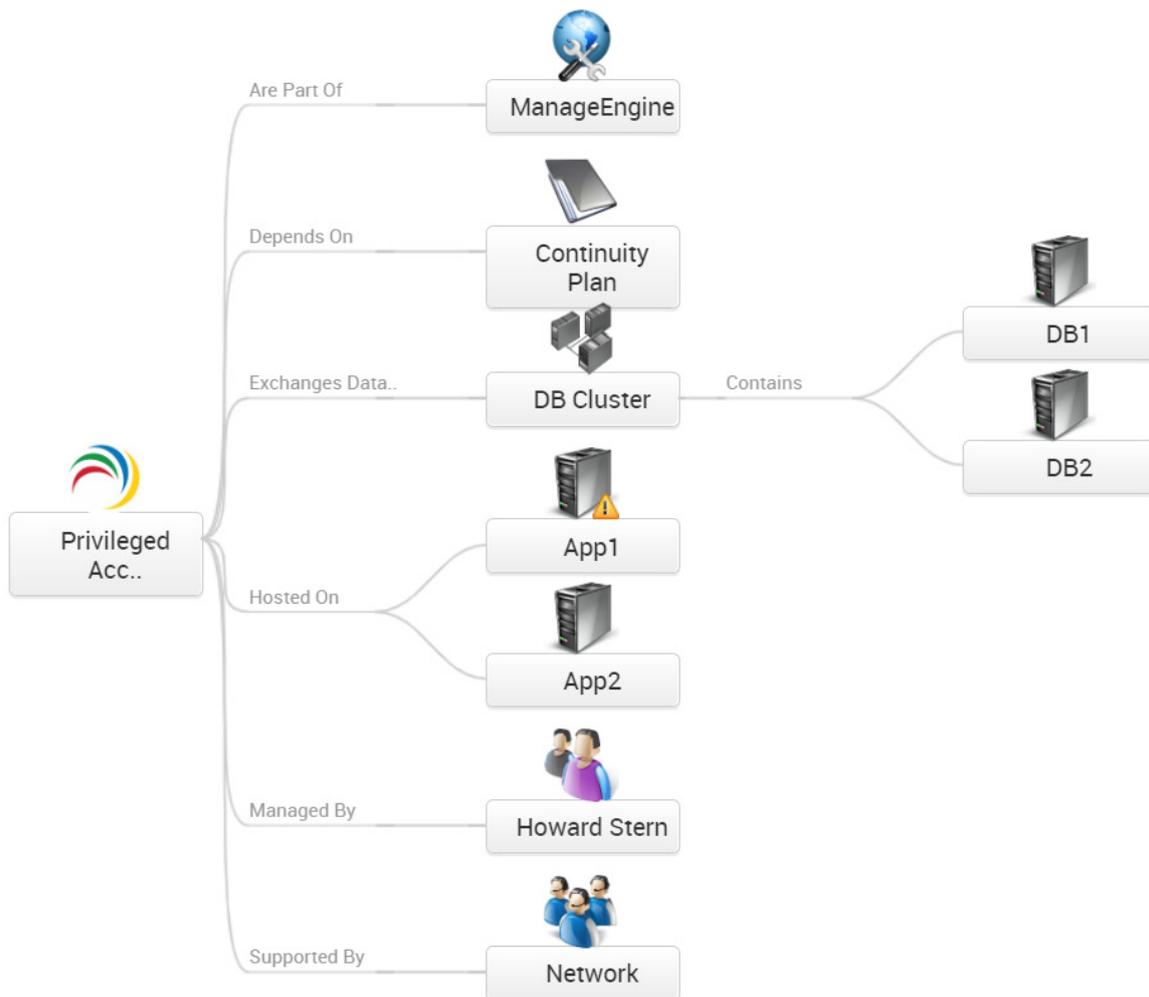
Service relationship with continuity plan

- ServiceDesk Plus supports creating preventive maintenance tasks using which a request to test the continuity plan can be created and assigned to appropriate IT personnel at planned intervals.

Preventive maintenance schedule

- As part of the change/release management process in ServiceDesk Plus, testing the continuity plan can be made a mandatory task for all major changes. The cause, impact, and recovery when the continuity plan has been invoked can be

OpManager Plus and Applications Manager

- When the continuity plan is invoked, OpManager Plus and Applications Manager can help monitor the service and service components availability, health, and
performance. The monitored data can be analyzed to identify deficiencies and risks to continuity based on various health and performance metrics.

OpManager	NetFlow	NCM	OpUtils	Firewall
System	Search Report	Hardware Inventory Report	Unused IP Addresses	Custom Report
Health and Performance	Report Profiles	Firmware Inventory	Reserved-Static IP Addresses	Firewall Reports
Availability and Response	Forensics	Device Inventory	IP Usage Summary	Proxy Reports
Inventory	Consolidated Report	Network Health Status	Switches by Usage	Policy Overview
WAN RTT Monitors	Compare Reports	Device Management Status	Switches by Scheduler	Policy Optimization
VoIP Monitors	Protocol Distribution	Device Audit	Switches by Vendor Name	Rule Cleanup
Virtual Servers Report	Inventory Report	Startup-Running Conflict	Switch Ports by ifSpeed	Rule Reorder
Storage Reports	Billing	Configuration Changes	Switch Ports by ifType	Rule Impact
Forecast Reports	Forecast	Configuration Change Trend	Device with Virtual IP	Standard
Nutanix Reports	Schedule	EOL/EOS Report	Stacked Port Details	Change Management
My Favorites	WAAS Dashboard	Compliance Report	Administratively Disabled Ports	Security Audit
Schedule Reports	WAAS Devices List	Configuration Analysis Report	Connected IP Details	Audit Logs
		Security Audit Report	Port by Operation Status Last Change Time	Rule Administration
		PCI Report	DHCP Reserved IP Addresses	Search Report

OpManager reports

- Monitor Group
- Trend Analysis Report
- Servers
- **Application Servers**
- Database Servers
- Web Services
- Web Servers
- URLs/ Web Apps
- Services
- Mail Servers
- ERP
- Middleware/Portal
- Virtualization
- Cloud Apps
- Converged Infrastructure
- Custom Monitors
- Capacity Planning
- End User Monitoring(EUM)
- Forecast Report

At a Glance Report
At a Glance Report of Application Servers

Availability Reports
Availability of Application Servers

Health Reports
Health of Application Servers

Response Time
Response Time of Application Servers

Memory Usage
JVM Details of Application Servers

JDBC Connection Usage
JDBC Connection Pool Usage of Application Servers

Thread Details
Thread Details of Application Servers

Session Details
HTTP Session of Application Servers

Request Throughput
Request Throughput of Application Servers

Web Application Request Throughput
Web Application Throughput of Application Servers

Select Attribute
---Select Attribute----

Reports in Applications Manager

8.7.3 Information security management

Addressed process requirement(s):

- The importance of conforming to the information security policy and its applicability shall be communicated to all interested parties.
- Information security controls shall be determined, implemented and operated to support the information security policy and address identified information security risks from both internal and external users.
- Monitor and review the effectiveness of information security controls and take necessary actions.
- Information security incidents shall be recorded, classified, prioritized, escalated if needed, resolved, and closed.
- Analyze the information security incidents by type, volume and impact on the SMS, services, and interested parties to identify opportunities for improve-

ManageEngine products that can help in implementing these process-

Endpoint Central

- The configuration management module helps you to publish the information security policy to all users of the organization through a logon Legal Notice. The policies can alsobe published through the ServiceDesk Plus self-service portal.
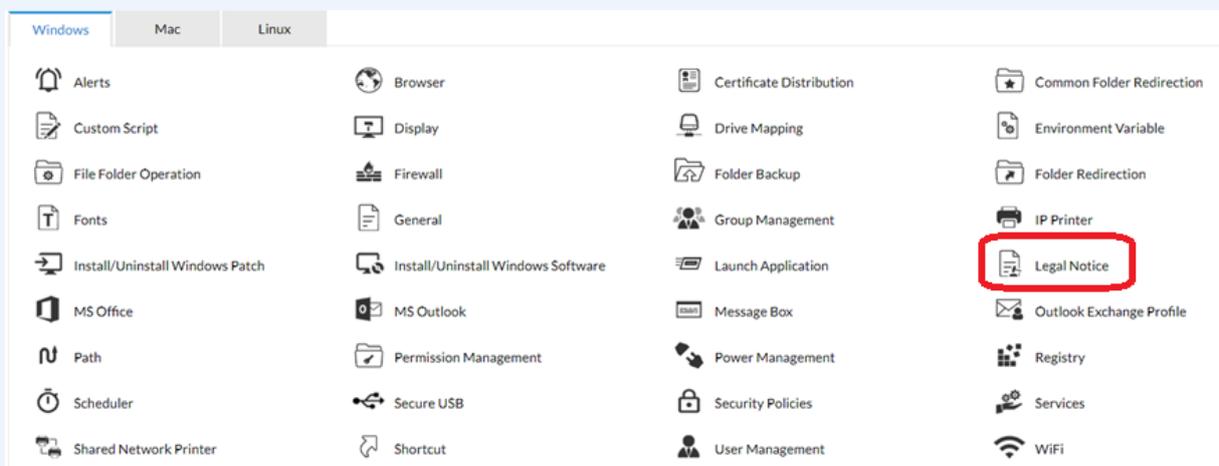
Endpoint Central: Manage configurations
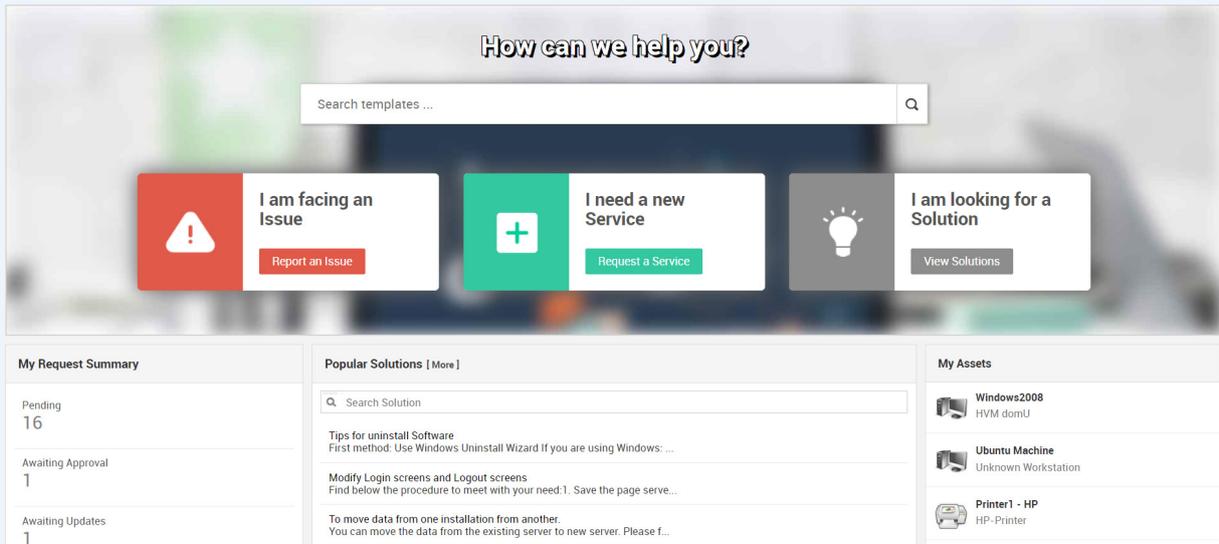
ServiceDesk Plus: Self-service portal

- Deploy the security controls required on endpoints like prohibiting specific software installation, blocking executables, blocking USBs, patching, recording the remote sessions, and securing mobile devices, browsers, and so on.
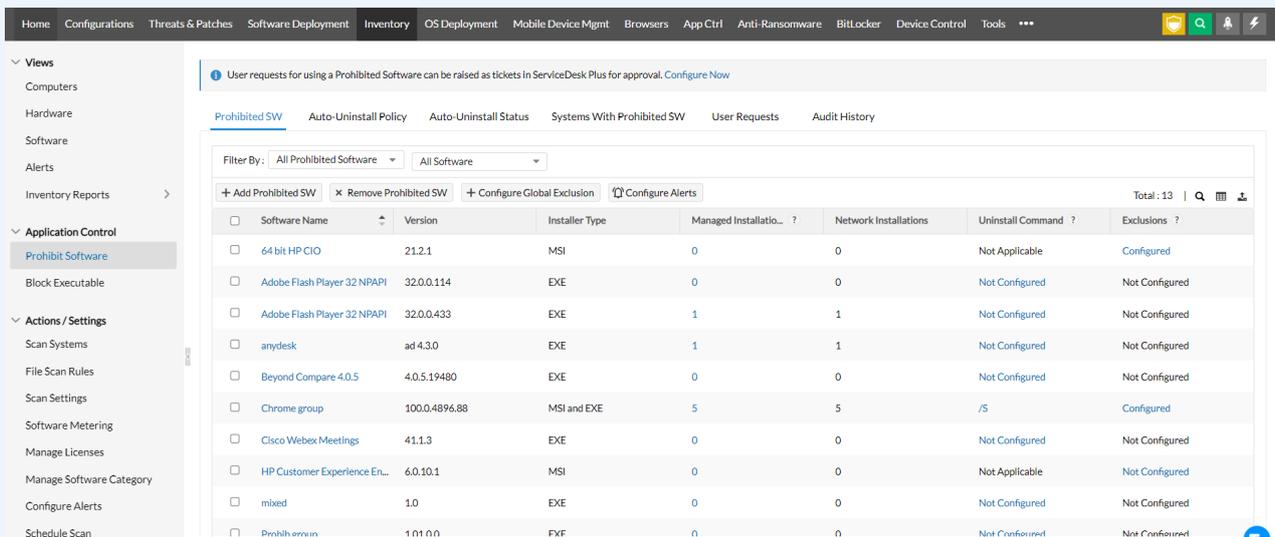
Endpoint Central: Control software and executable installation
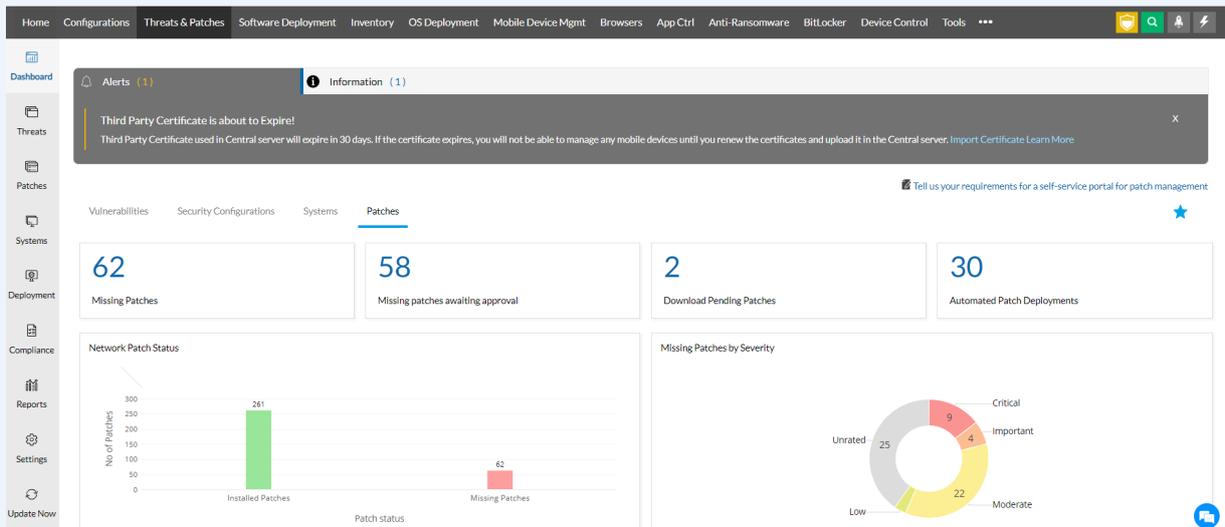
Endpoint Central: Comprehensive patch management

Endpoint Central: Recorded remote sessions
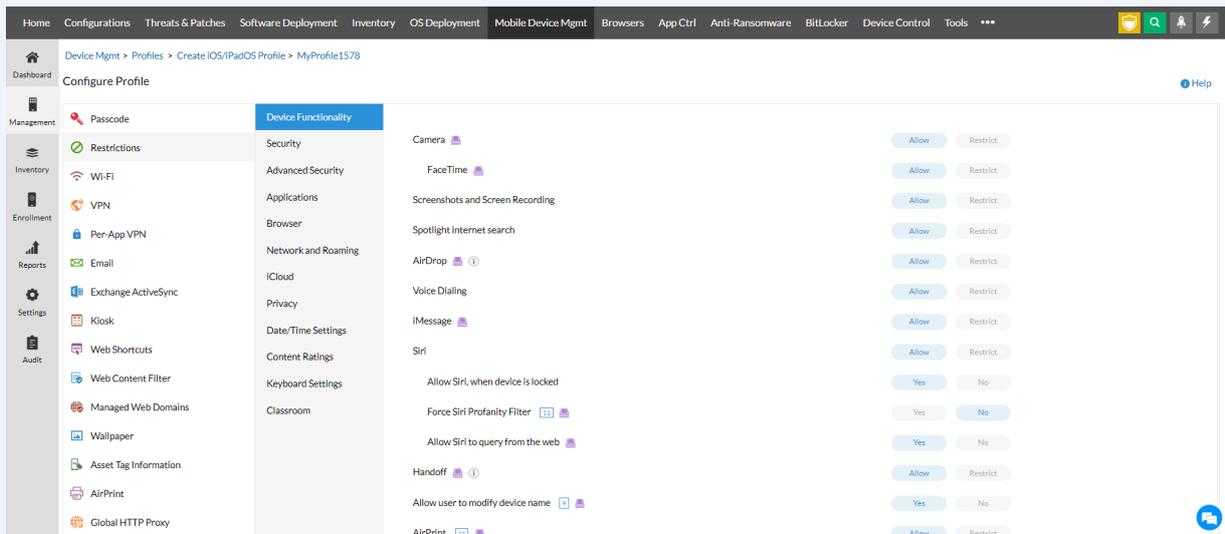
Endpoint Central: Securing mobile devices
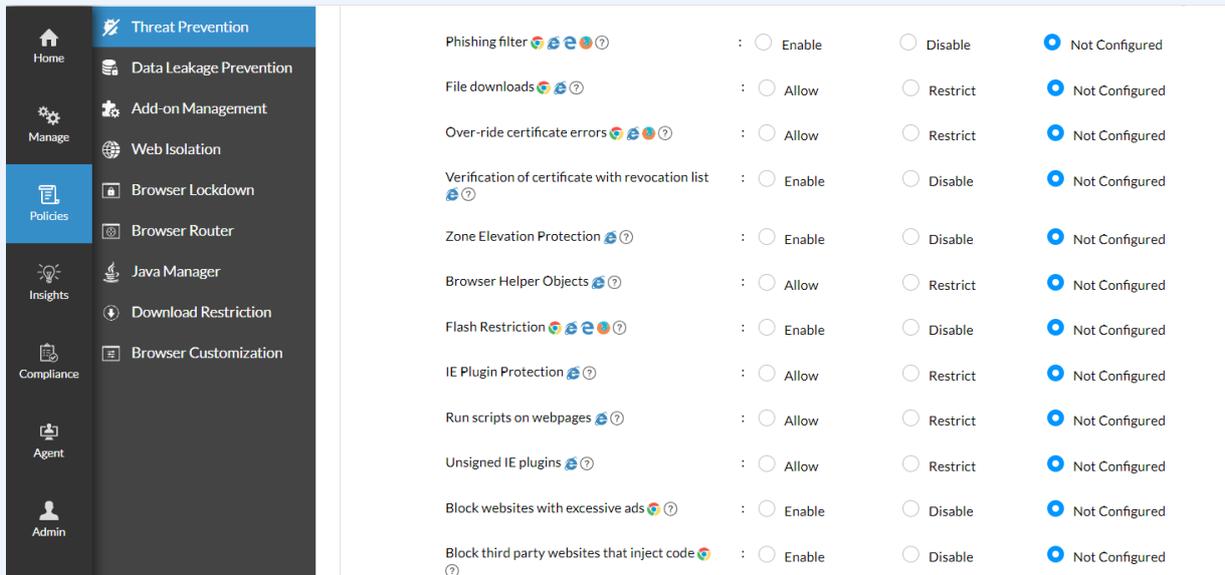
Browser risk management

AD360

- Deploy the security controls required for accessing and managing Active Directory, Exchange, and Microsoft 365 securely through the delegated capabilities. It also helps to deploy required controls for users to change/reset the password, unlock accounts through multiple identity verification methods, and implement multi-factor authentication for users to log in to their machines.

License   📁 AD Explorer

Search AD Objects

| Home | Management | Reports | Office 365 | Delegation | Workflow | Automation | Admin | Backup | Support |

Domain Settings

Requests

Create Request
All Requests

Workflow Delegation

Requesters
Workflow Technicians
Requester Roles

Configuration

Business Workflow
Assigning Rules

Business Workflow

Define an order of execution for important administrative tasks. Learn more...

Create Request

Workflow Name   [Enter a name]

Description   [Enter a description]

Workflow Stages

Requester — The one who raises a request for a particular action. [Configure]

☑ **Reviewer** — The one who assesses the request, weighs its pros and cons, and offers recommendations. [Configure]   No. of Reviewers: 1

☑ **Approver** — The one who possesses the authority to finalize an action. [Configure]   No. of Approvers: 1

☑ **Executor** — The one who ex... the approved ac... [Configure]

Create Workflow   Cancel

1-4 of 4   5

Action	Workflow Name	Description	Workflow Stages
✎ 🗑	Default business workflow	This is a predefined workflow present in the product.	Requester → Executor
✎ 🗑	User onboarding workflow	This workflow will be used while processing the request for user account creation.	Requester → Reviewers: 1 → Executor
✎ 🗑	Stale accounts cleanup workflow	This workflow will be used while processing stale accounts cleanup.	Requester → Reviewers: 2 → Executor
✎ 🗑	User password reset workflow	This workflow will be used while processing password reset requests.	Requester → Reviewers: 2 → Approver: 2 → Executor

Commit changes in AD on approval

| ☐ AD Management | ☐ AD Reports | ☐ Administration | ☐ Office 365 | ☐ Backup |

User Management
Computer Management
Group Management
Contact Management
Mailbox Management
OU Management
File Server Management
GPO Management

Bulk User Management

☐ **Create Users**   User Attribute Privileges
   ☐ Create Single User
   ☐ Create Bulk Users

☐ **Modify Users** ⓘ
   ☐ Modify Single User
   ☐ Modify Bulk Users

☐ **User Templates**
   ☐ User Creation Templates
   ☐ User Modification Templates

Bulk User Modification   ☐ Deny Bulk Modification

☐ **General Attributes**
☐ Reset Password
☐ Group Attributes
☐ Unlock Users
☐ Move Users
☐ Delete Users
☐ Account Attributes
☐ Restore Deleted Users
☐ Address/Organization Attributes
☐ Naming Attributes
☐ Profile Attributes
☐ Move/Delete Home folders
☐ Contact Attributes
☐ Modify Custom Attributes

☐ **Exchange Attributes**
☐ Create/Archive MailBox
☐ Modify SMTP Address
☐ Set MailBox Rights
☐ Delivery Options
☐ Naming Attributes
☐ Exchange Features
☐ Auto Reply
☐ Delivery Restrictions
☐ Storage Limits
☐ Migrate Mailbox
☐ Exchange Offline Address Book
☐ Disable/Delete User MailBox
☐ Exchange Policies

☐ **Terminal Services**
☐ Profile Attributes
☐ Remote Control Attributes
☐ Session Attributes
☐ Environment Attributes
☐ Move/Delete TS Home folders
☐ Dial-in

Delegate access for AD management

User Reports
Password Reports
Group Reports
Computer Reports
Exchange Reports
Contact Reports
Terminal Service Reports
GPO Reports
OU Reports
NTFS Reports
Security Reports
Other Reports
Compliance Reports
G Suite Reports
Custom Reports

Compliance Reports

SOX
All Users
All Groups
All Computers
All Contacts
All OUs
All GPOs & Linked AD Objects
Office 365 Users

HIPAA
Recently Logged On Users
Recent Logon Failures
Real Last Logon
Users With Terminal Server Access
Recently Created Users
Recently Modified Users

PCI
Recently Logged On Users
Recent Logon Failures
Real Last Logon
Locked-out Users
Users in Groups
Shares in the Servers
Permissions for Folders

FISMA
Recent Logon Failures
Real Last Logon
Users with Password Never Expires
Password Changed Users
Recently Created Users
Recently Modified Users

GLBA
Recently Logged On Users
Recent Logon Failures
Real Last Logon
Users with Password Never Expires
Password Changed Users
Security Groups

GDPR
Shares in the Servers
Permissions for Folders
Folders accessible by Accounts
Server Permissions
Subnet Permissions
Servers accessible by Accounts
Subnets accessible by Accounts

Compliance reports for AD management
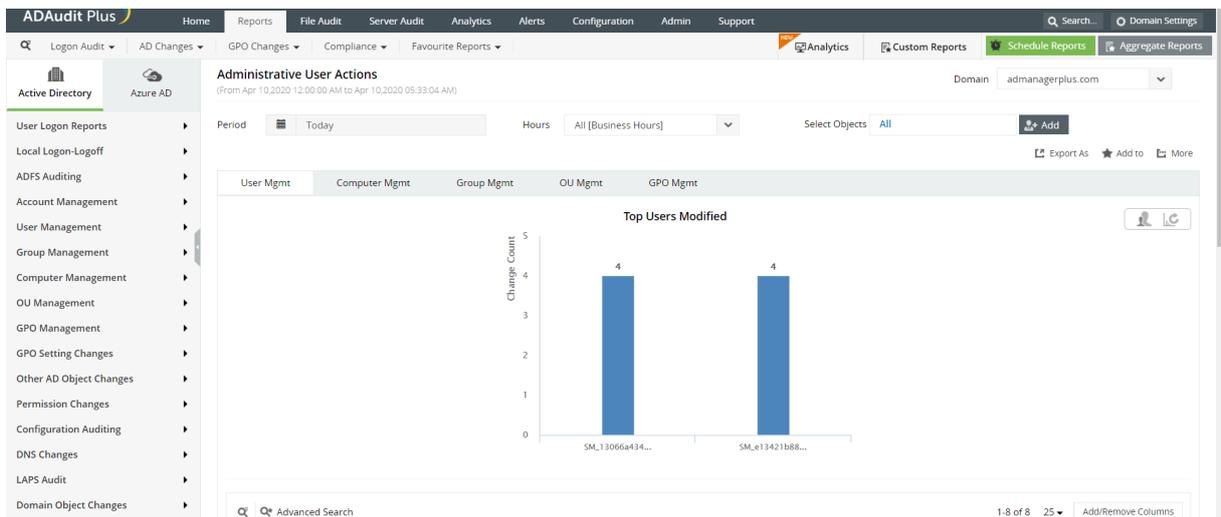
*AD and file server change auditing*
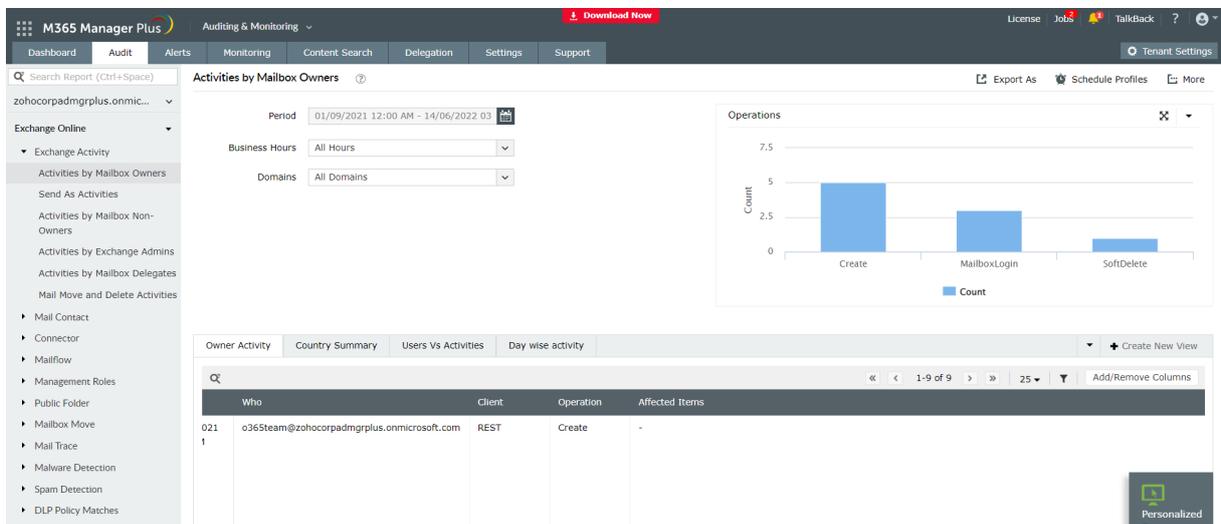
M365 management auditing and reporting

Securely self manage passwords and accounts

M365 management auditing and reporting

Securely self manage passwords and accounts

Exchange auditing and reporting

PAM360

- Deploy the required controls on privileged access to both internal and external users for any service component like network devices, servers, databases, etc. The passwords of the service components can be stored securely and access to them can be granted based on approval. It records the privileged session and has the capability to provide just-in-time privilege escalation as well.
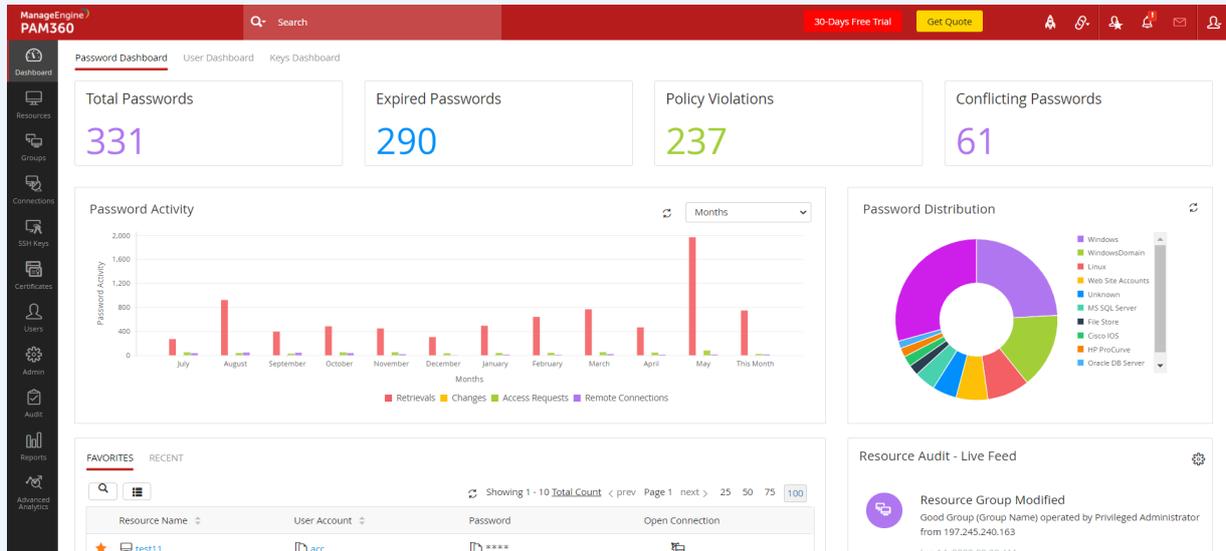
Secured privileged password management

SSL/SSH key management

Activity audit: Recorded sessions
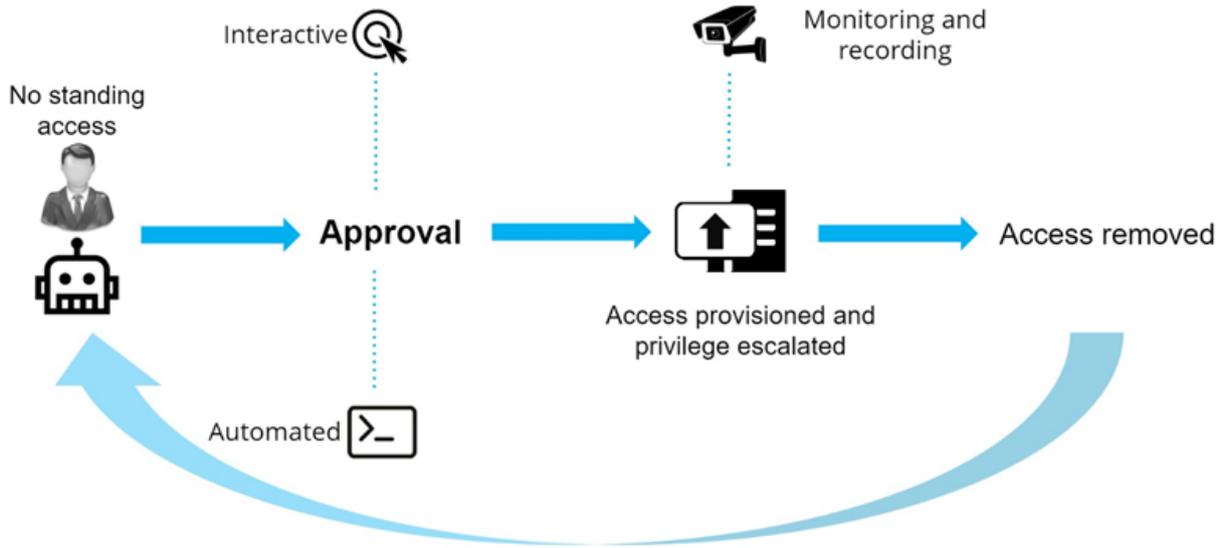
Just-in-time privilege escalation

- The stored password can be changed post access or periodically using the configured password policy. It provides reporting on ISO 27001 as well by de-
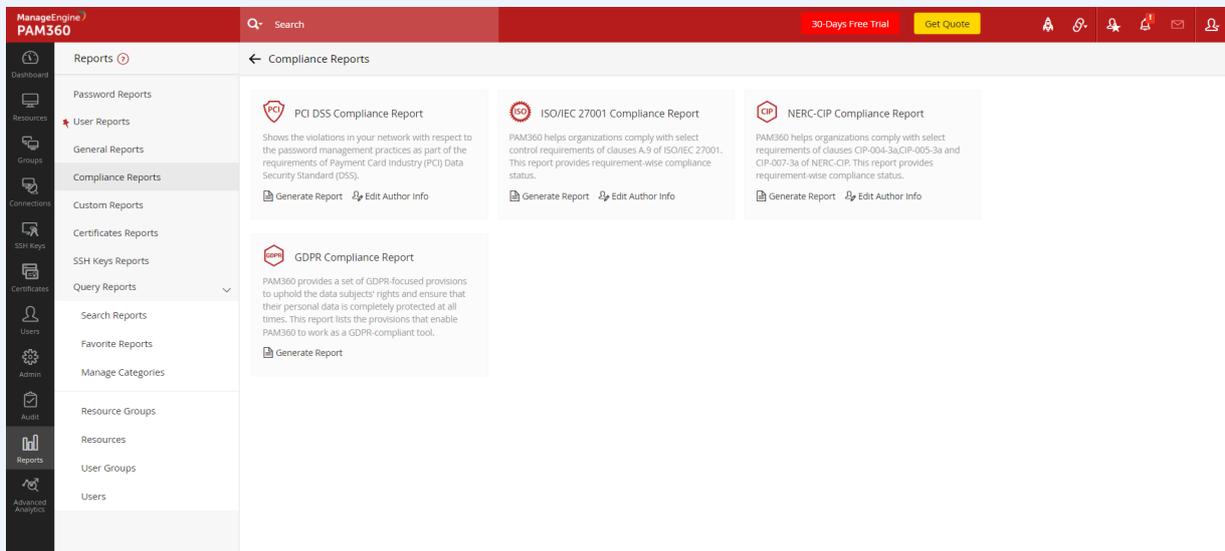
Compliance reports

OpManager Plus

- The Network Configuration Manager component of OpManager Plus helps to track whether all the network devices are compliant based on a set of policies.

Compliance check for network devices

- The Firewall Analyzer component helps you to analyze firewall logs for threat and risks on firewalls.

Firewall log management

ISO on 2020-04-03 06:54

This assessment is based on the ISO(27001:2013) Security Standard for firewalls. For more information, please visit http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

75% Compliant
Recommendation:
Please ensure that you satisfy all the compliance requirement

Failed Count2
9.4 Firewall Access Control
13.1.2 Explicit deny rule

** Some requirements need to be manually verified.:   more...

PCI DSS on 2019-10-16 00:06

This assessment is based on the PCI Data Security Standard, Version 3.0, and covers all control items that address Firewall policy issues. For more information, please visit https://www.pcisecuritystandards.org

62% Compliant
Recommendation:
Please ensure that you satisfy all the compliance requirement

Failed Count3
1.1.7 Periodic Review of Rule Sets
1.2.1 b Explicit Deny rule
2.3 Encrypt Administrative Access

** Some requirements need to be manually verified.:   more...

NIST on 2018-09-17 21:16

This assessment is based on the NIST Standard of compliance. For more information, please visit http://www.identity-theft-awareness.com/NIST-security-compliance.html

77% Compliant
Recommendation:
Please ensure that you satisfy all the compliance requirement

Failed Count2
2.1 Explicit Deny rule
2.10.1 Explicit Deny rule For Incoming TCP,UDP and ICMP traffic

** Some requirements need to be manually verified.:   more...

NERC-CIP on 2019-08-28 14:37

This assessment is based on the NERC-CIP Standards oversight by the Federal Energy Regulatory Commission for version 3. Please visit http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

62% Compliant
Recommendation:
Please ensure that you satisfy all the compliance requirement

Failed Count3
CIP-003-R5.1 Security Management Controls
CIP-005-R2.1 Explicit Deny rule
CIP-007-R2.2 Explicit Deny rule

** Some requirements need to be manually verified.:   more...

Firewall log management

Log360

- Audit the changes and activities on Active Directory, file servers, network devices, servers, applications, databases, workstations, Microsoft 365, Exchange, AWS, Azure, etc., which serves as a evidence against the implemented controls and also to evaluate the effectiveness and to identify opportunities for improvement.

Integrated Compliance Management

Real-Time Active Directory Change Auditing

File Integrity Monitoring

SQL And IIS Auditing

Network Device Auditing

Office 365 Auditing

Privileged User Activity Monitoring

Exchange Auditing

Data Visibility And Security

Log360 UEBA

Active Directory Reporting

Log 360: Comprehensive SIEM solution

Events overview
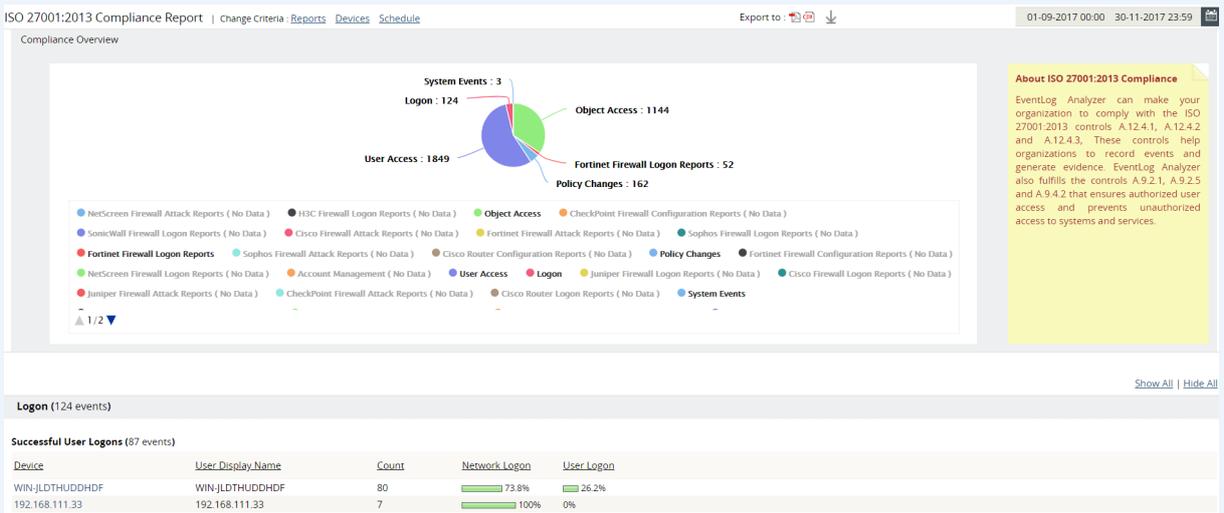
Compliance reports

ServiceDesk Plus

- Information security incidents can be logged in ServiceDesk Plus as a separate type of incident and can follow its SLA and process. By default, ManageEngine products can be integrated with ServiceDesk Plus through the possible incident creation methods like email or API to report on security incidents. Reporting helps you to analyze incidents and identify opportunities for improvement.
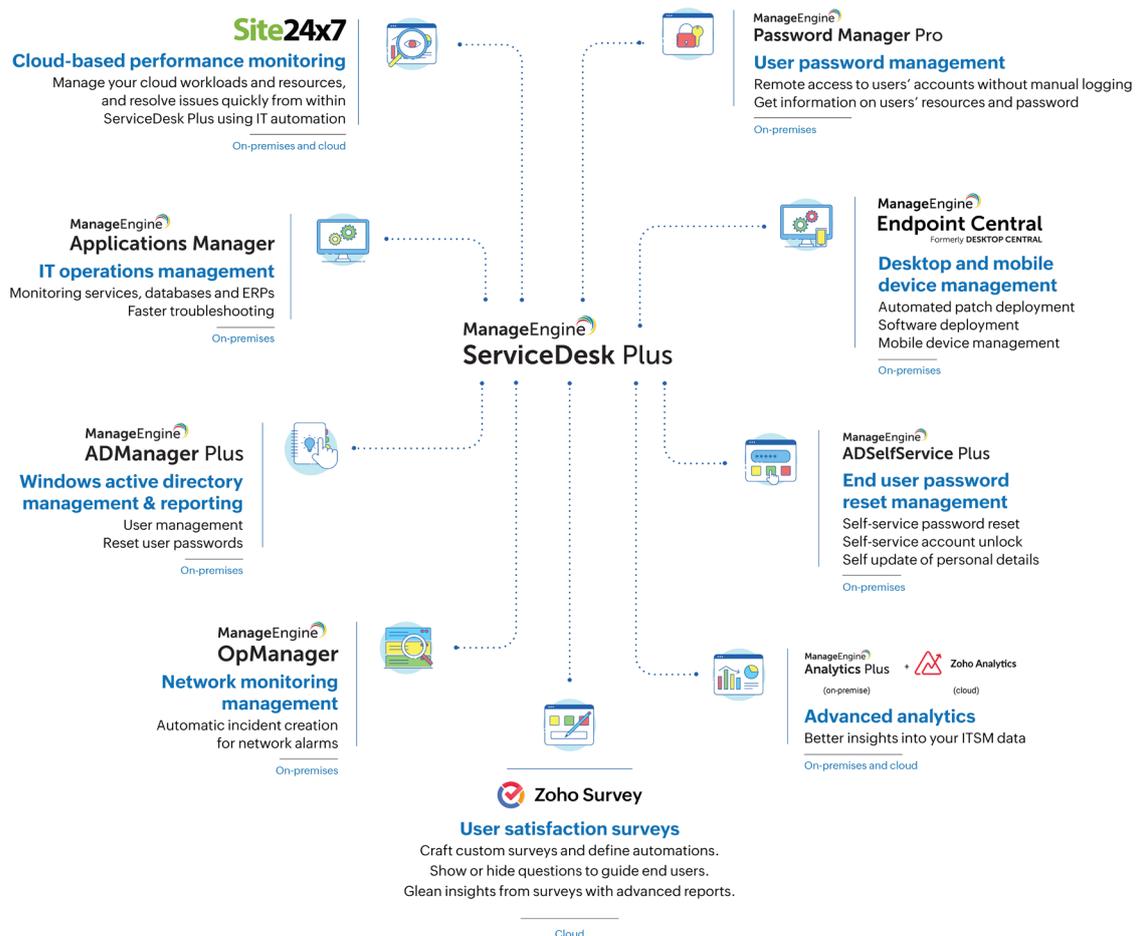
Out-of-the box integrations

Clause 9:
Performance evaluation

9.4 Service reporting

Addressed process requirement(s):

- Reports on the performance and effectiveness of the services shall be produced and shall include trends.

- The reports required are specified in the relevant clauses. Additional reports can also be produced.

ManageEngine product that can help in implementing these processes:

- All the proposed ManageEngine products by default provide reporting based on the functionalities they offer. They also store and maintain the trend based on the configured time period. Apart from the default reports, ManageEngine products offer options to create custom reports based on the need, and extensive reporting is possible through the Advanced Analytics.

Reporting using advanced analytics

Bringing IT together

ManageEngine crafts comprehensive IT management software for all your business needs.
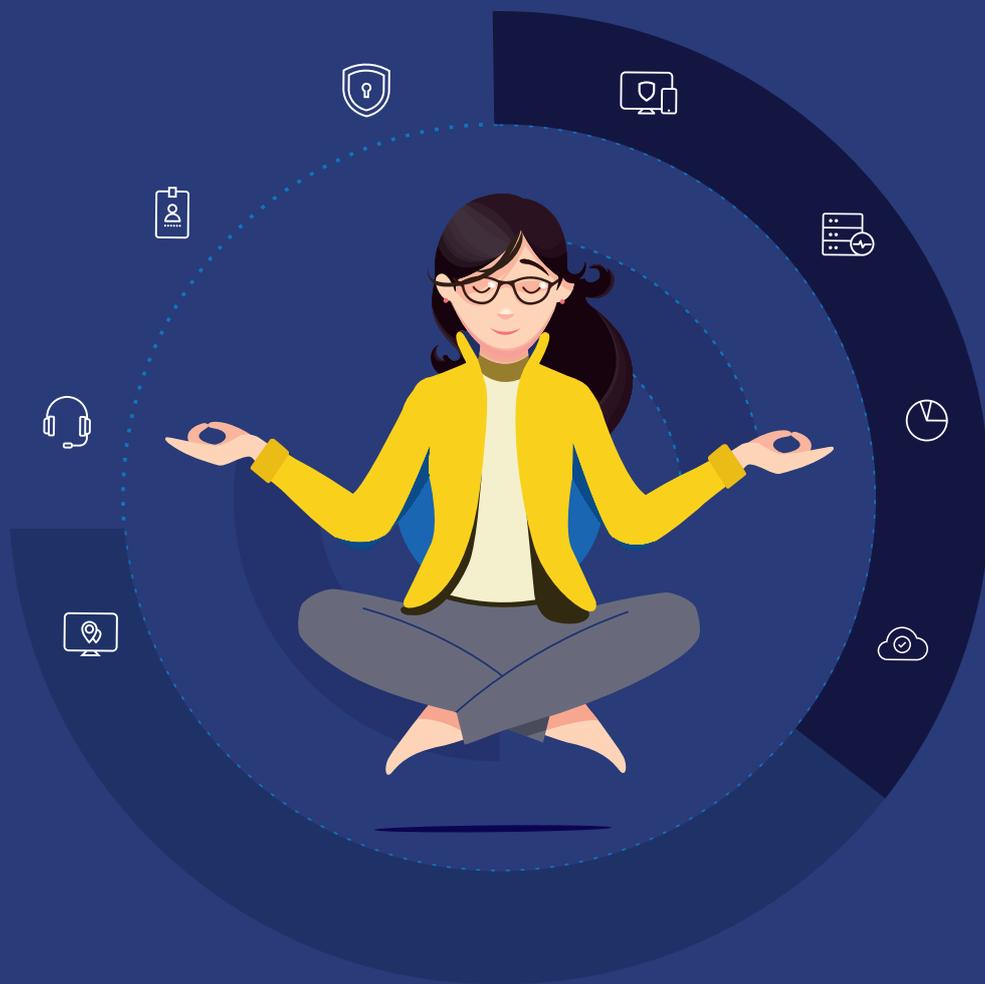
Available for

Enterprise IT Managed service providers (MSPs) as
Self hosted on-premises
Self hosted in public cloud (AWS, Azure)
Cloud (SaaS)

Enterprise service management

- Full-stack ITSM suite

- IT asset management with CMDB

- Knowledge base with user self-service

- Built-in and custom workflows

- Orchestration of all IT management functions

- Service management for all departments

- Reporting and analytics

Identity and access management

- Identity governance and administration

- Privileged identity and access management

- AD and Azure AD management and auditing

- SSO for on-premises and cloud apps with MFA

- Password self-service and sync

- Microsoft 365 & Exchange management and auditing

- AD & Exchange -backup and recovery

- SSH and SSL certificate management

Security information and event management

- Unified SIEM for cloud and on-premises

- AI driven user and entity behavior analytics

- Firewall log analytics

- Data leakage prevention and risk assessment

- Regulatory and privacy compliance

Unified endpoint management

- Desktop and mobile device management

- Patch management Endpoint device security

- OS and software deployment

- Remote monitoring and management

- Web browser security

- Monitoring and control of peripheral devices

IT operations management

- Network, server, and application performance monitoring

- Bandwidth monitoring with traffic analysis

- Network change and configuration management

- Application discovery and dependency mapping

- Cloud cost and infrastructure monitoring

- End-user experience monitoring

- AIOps

Advanced IT analytics

- Self-service IT analytics

- Data visualization and business intelligence for IT

- Hundreds of built-in reports and dashboards

- Instant, flexible report creation

- Out-of-the-box support for multiple data sources

About ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need — more than 90 products and free tools — to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use. You can find our on-premises and cloud solutions powering the IT of over 280,000 companies around the world, including nine of every ten Fortune 100 companies.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize opportunities in the future.

ManageEngine

For more information:

www.manageengine.com

sales@manageengine.com

ManageEngine