# 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).

## Cyber Essentials:

Cyber Essentials is a UK government-backed scheme designed to help organizations protect themselves against common cyber threats. It outlines a set of basic cybersecurity controls that all organizations can implement to mitigate risks and demonstrate a commitment to cybersecurity.

## CCPA:

CCPA is a data privacy law specific to the processing of personal information of California residents that requires businesses to protect their personal information and provides privacy. ManageEngine's offerings have privacy features that enable it's users to comply with the CCPA, and ManageEngine's processing of its Californian customer's data adheres to requirements of the CCPA.

## SOC 2 + HIPAA:

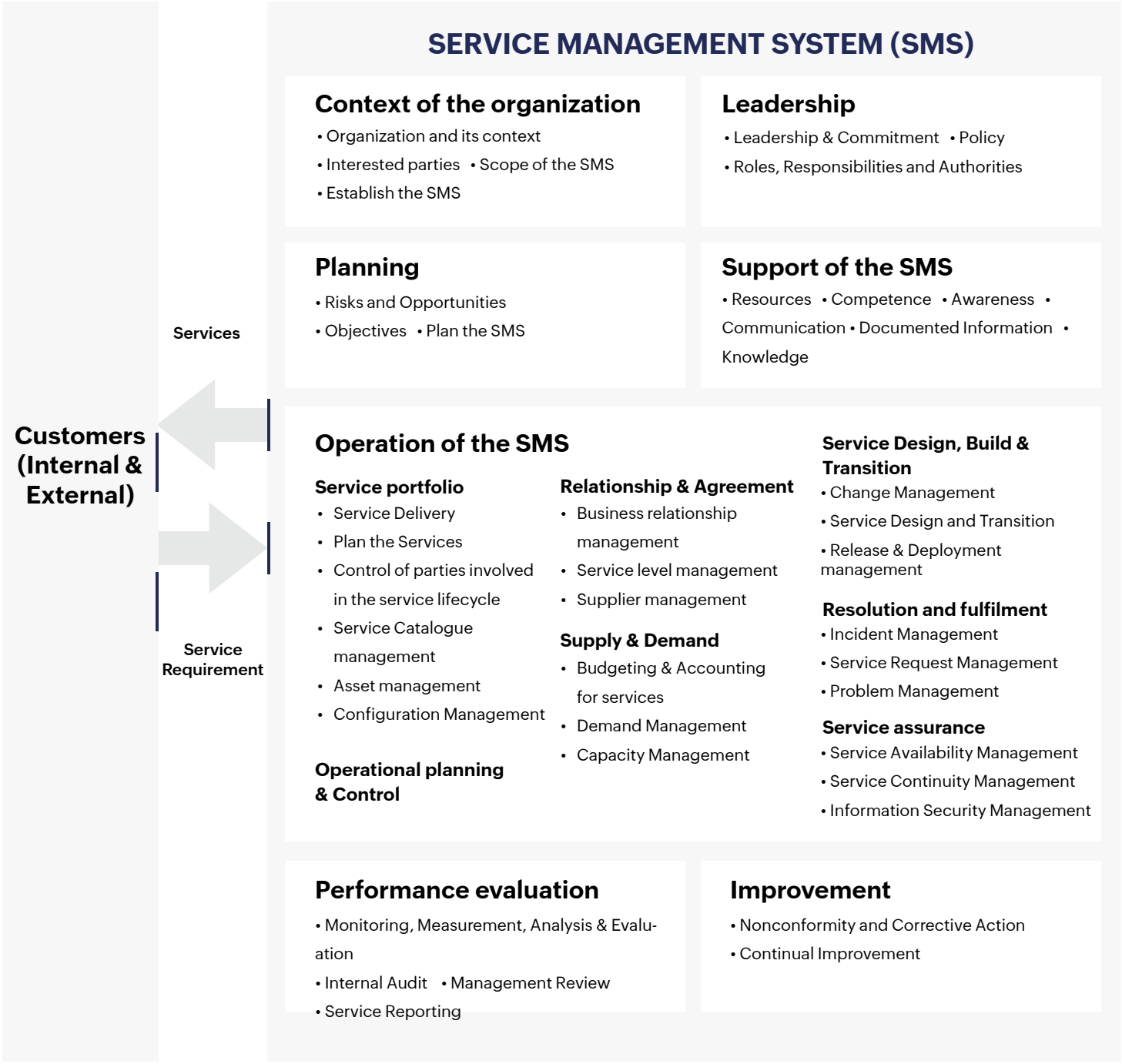
An independent third-party audit firm has examined the description of the system related to Application Development, Production Support and the related General Information Technology Controls for the services provided to customers, from Zoho offshore development center, based on Security, Privacy and breach requirements set forth in the Health Insurance Portability and Accountability Act ("HIPAA") Administrative Simplification. The responsibility of Zoho Corp. is limited to the extent it acts as a 'Business Associate'. ManageEngine is a division of Zoho Corp.

## 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 requirement document to help with conformance.




*The mandatory requirements mentioned in ISO 20000-1 that need to be fulfilled for certification*

*Clause 8:*

# Operation of the service management system

# 8.2 Service portfolio

## 8.2.4 Service catalog management

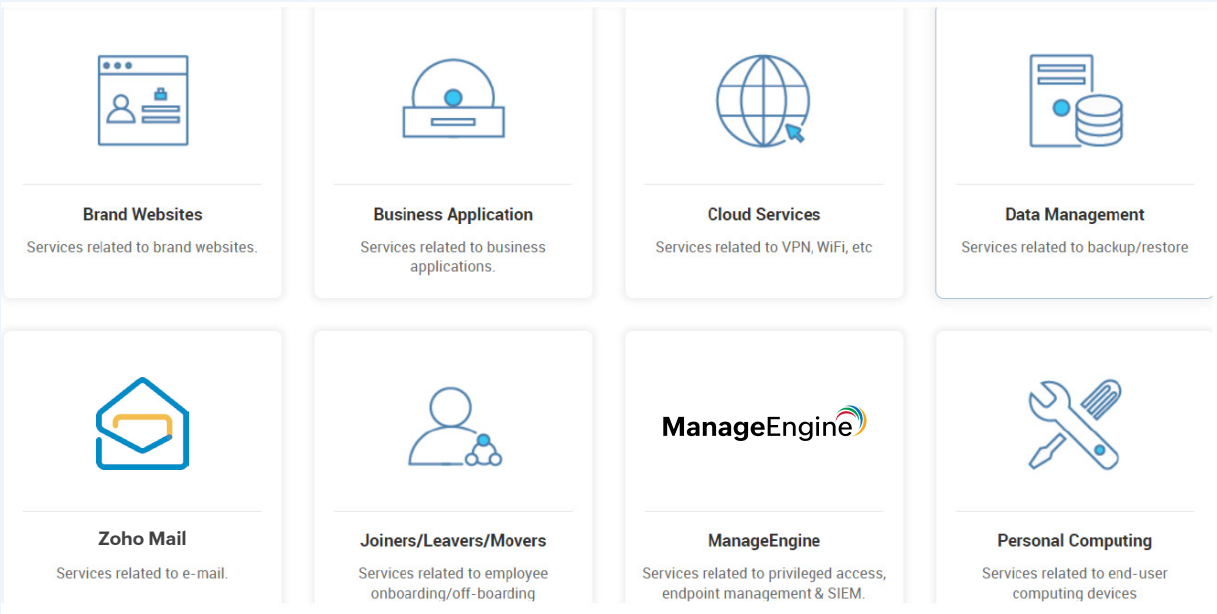
### Addressed process requirement(s):

- 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:

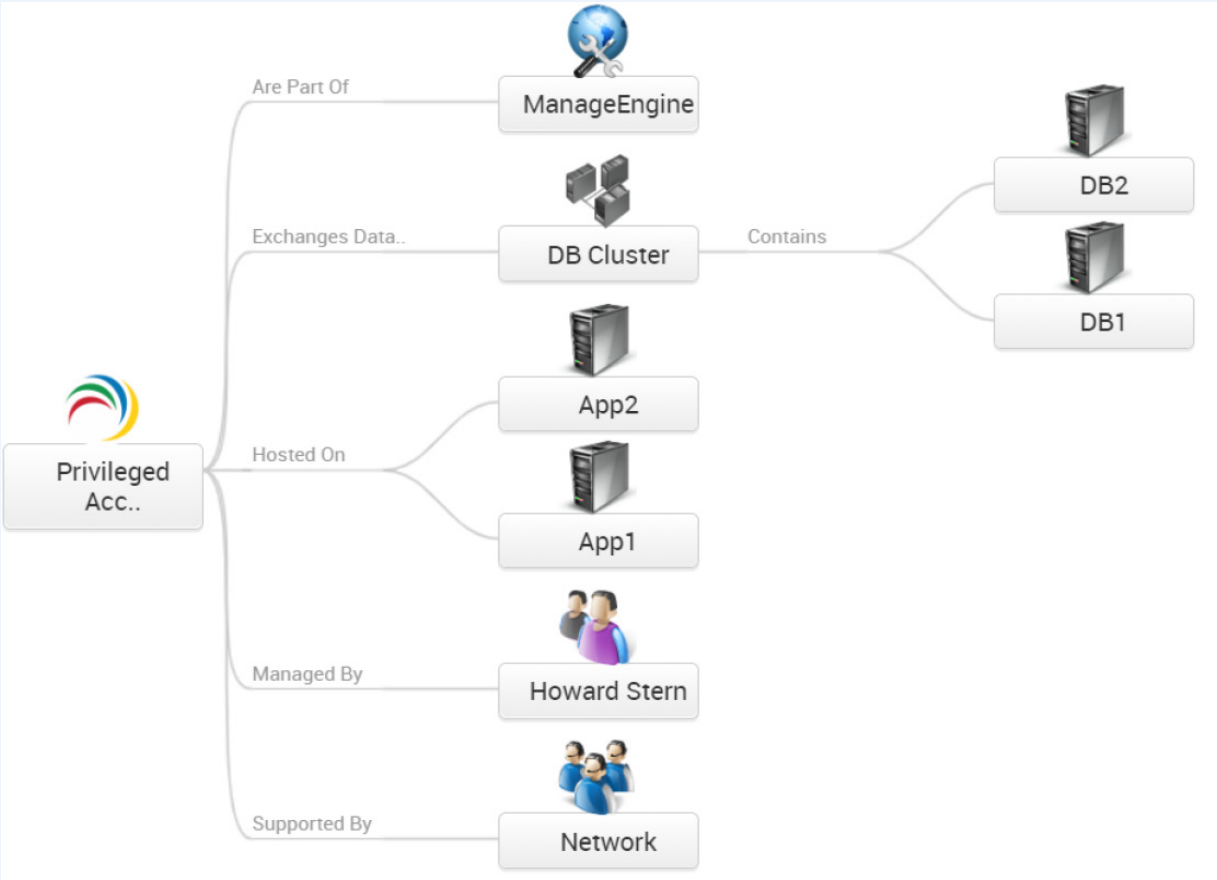
**ServiceDesk Plus**

- 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

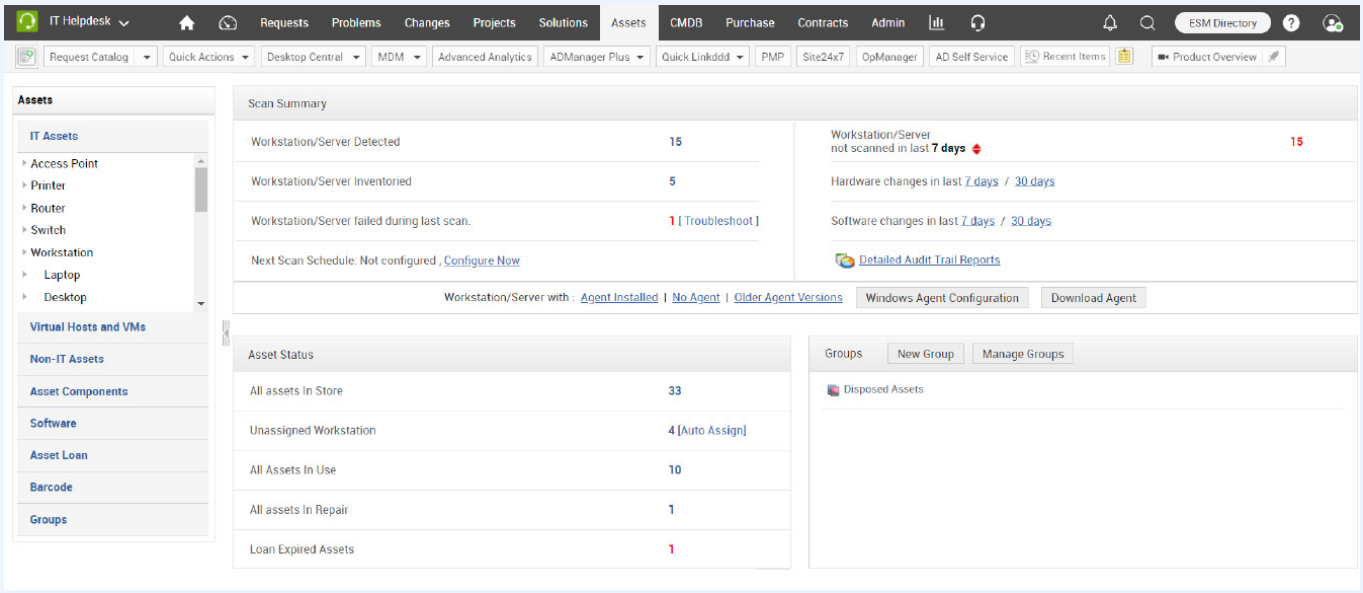
### Addressed process requirement(s):

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

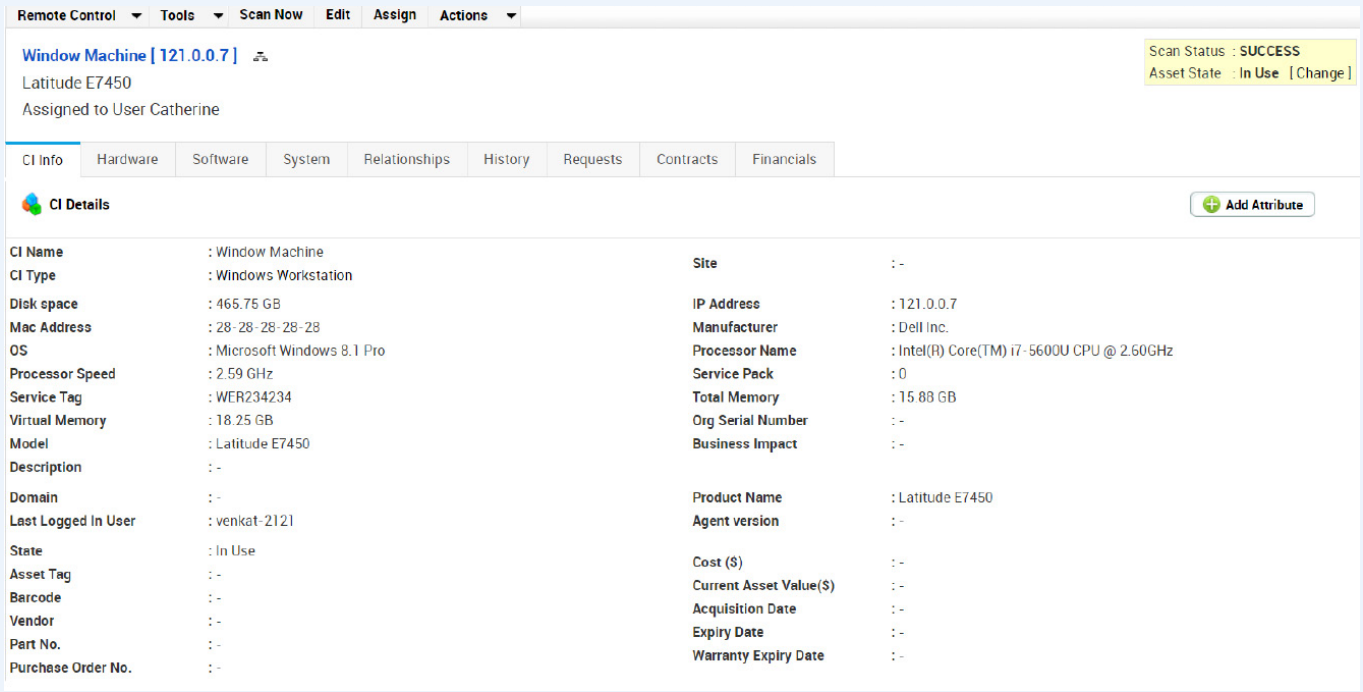
### ManageEngine product that can help in implementing this process:

**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

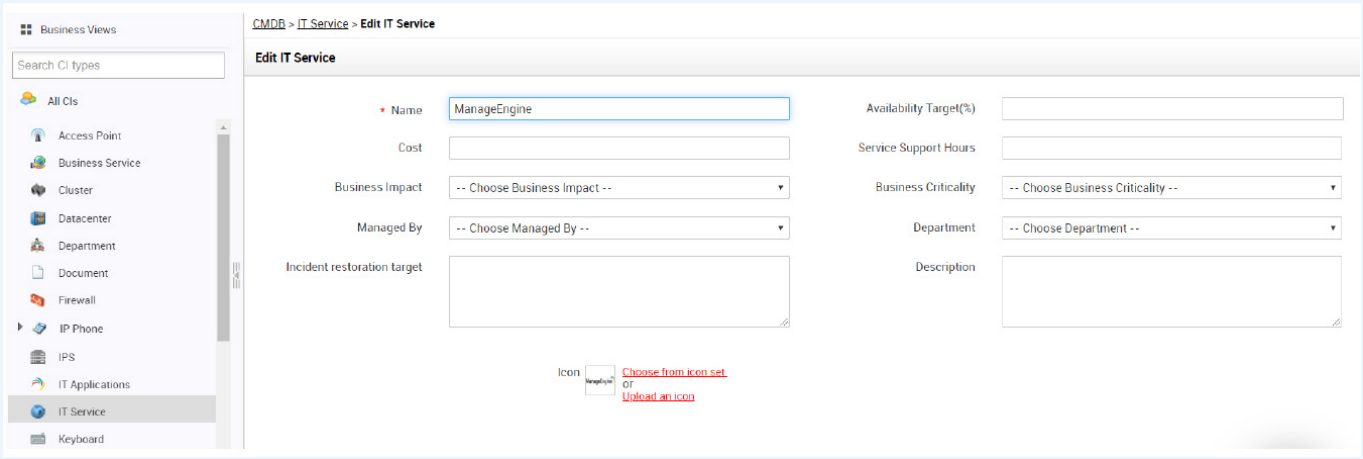
### Addressed process requirement(s):

- 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

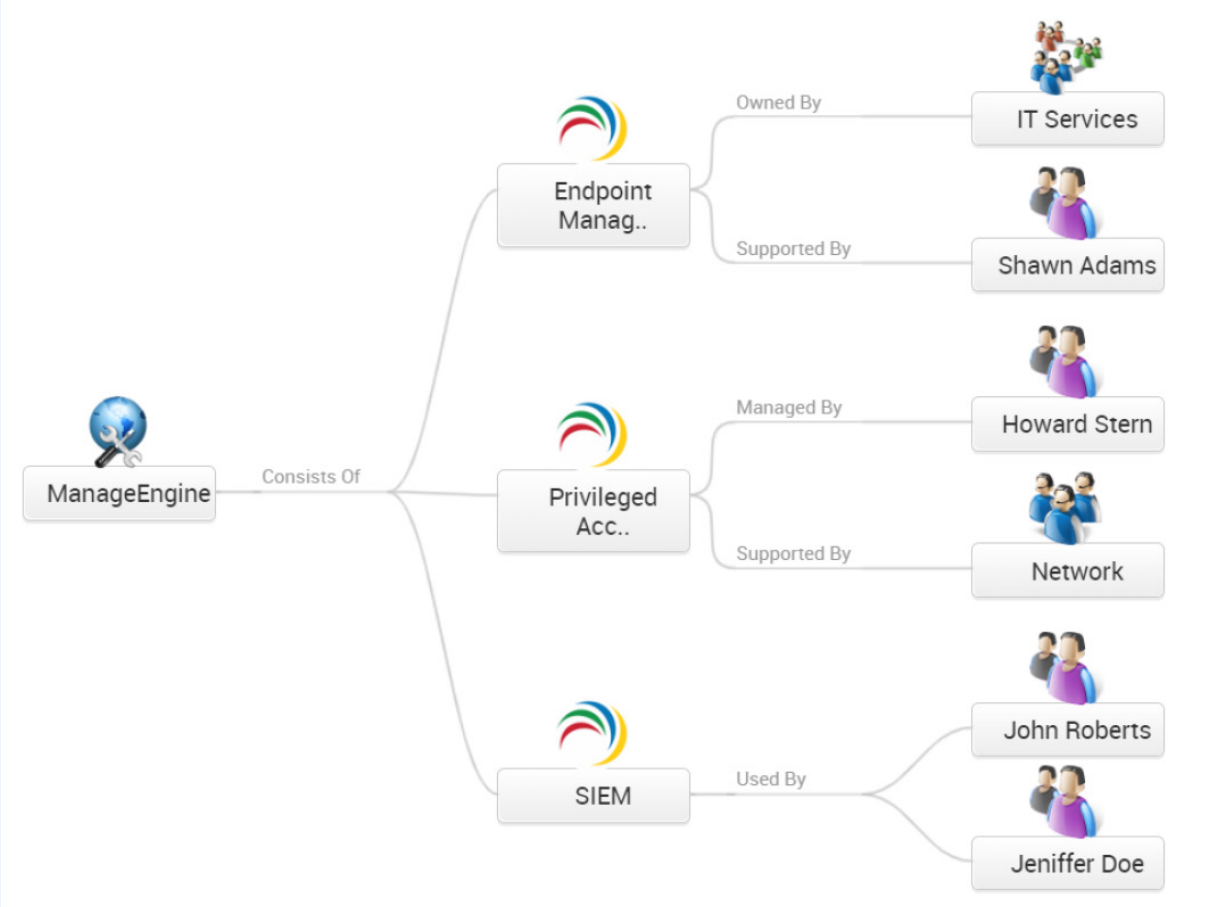
**Addressed process requirement(s):**

- 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, they should be escalated.

**ManageEngine product that can help in implementing these processes:**

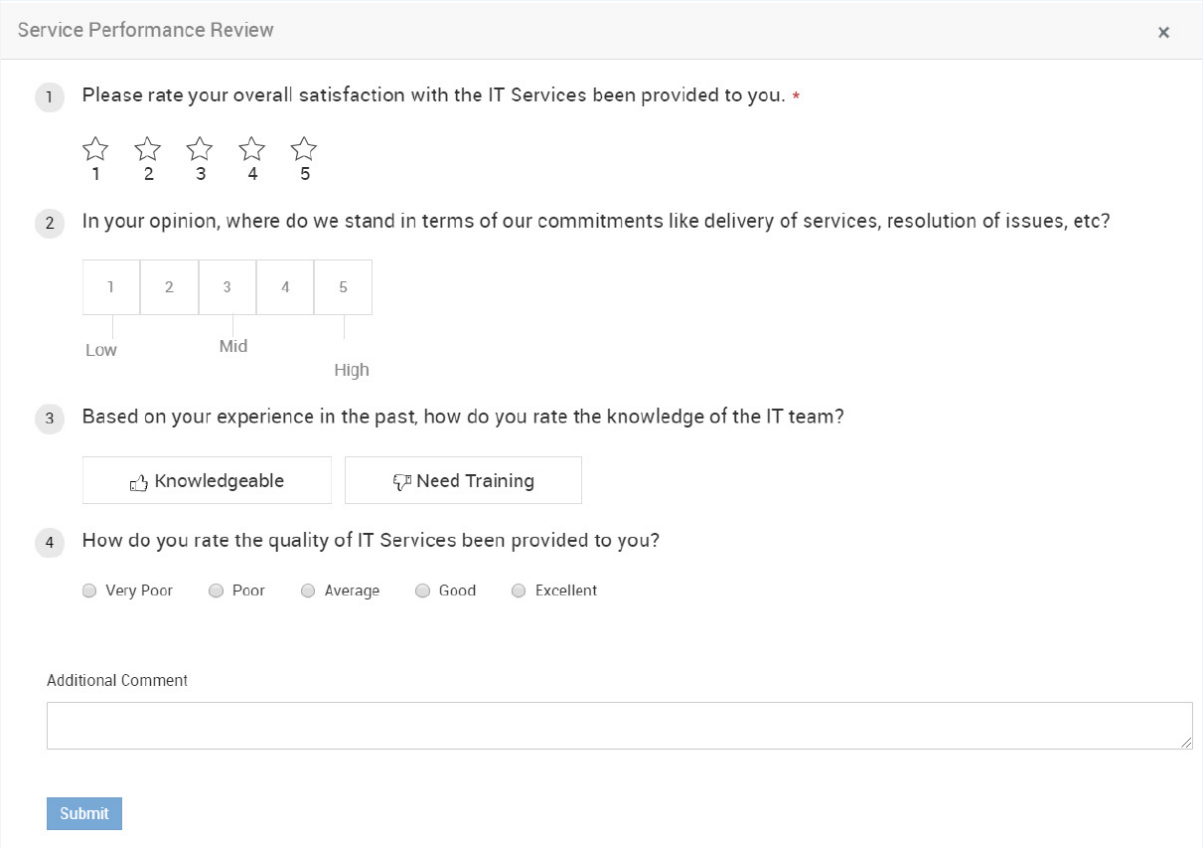
**ServiceDesk Plus**

- Visual relationships in the CMDB module document the details related to the services.



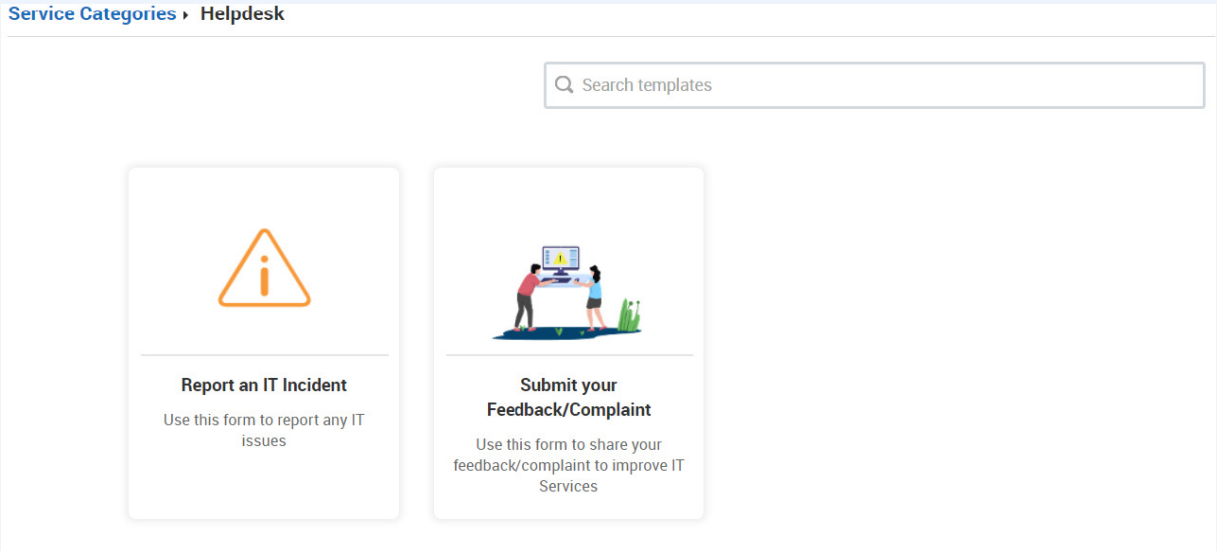

*Relationships with users mapped in the CMDB*

- 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

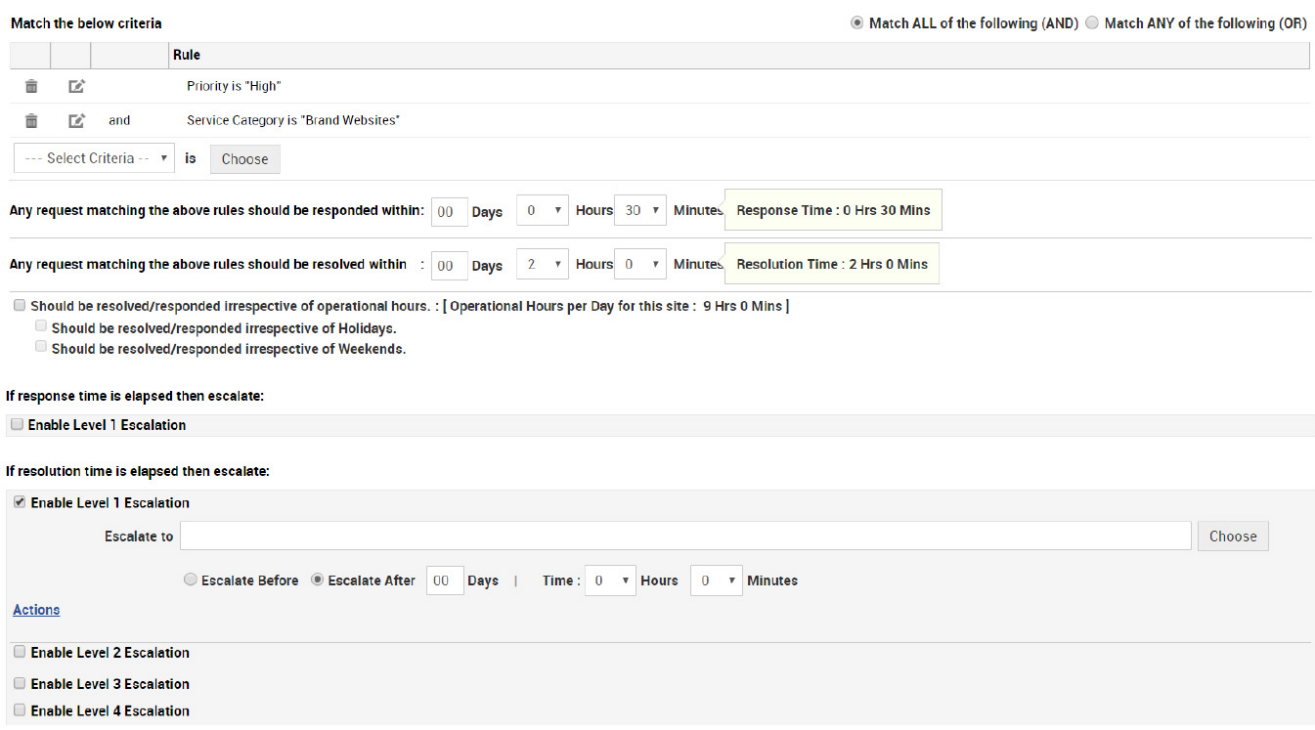
### Addressed process requirement(s):

- 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.

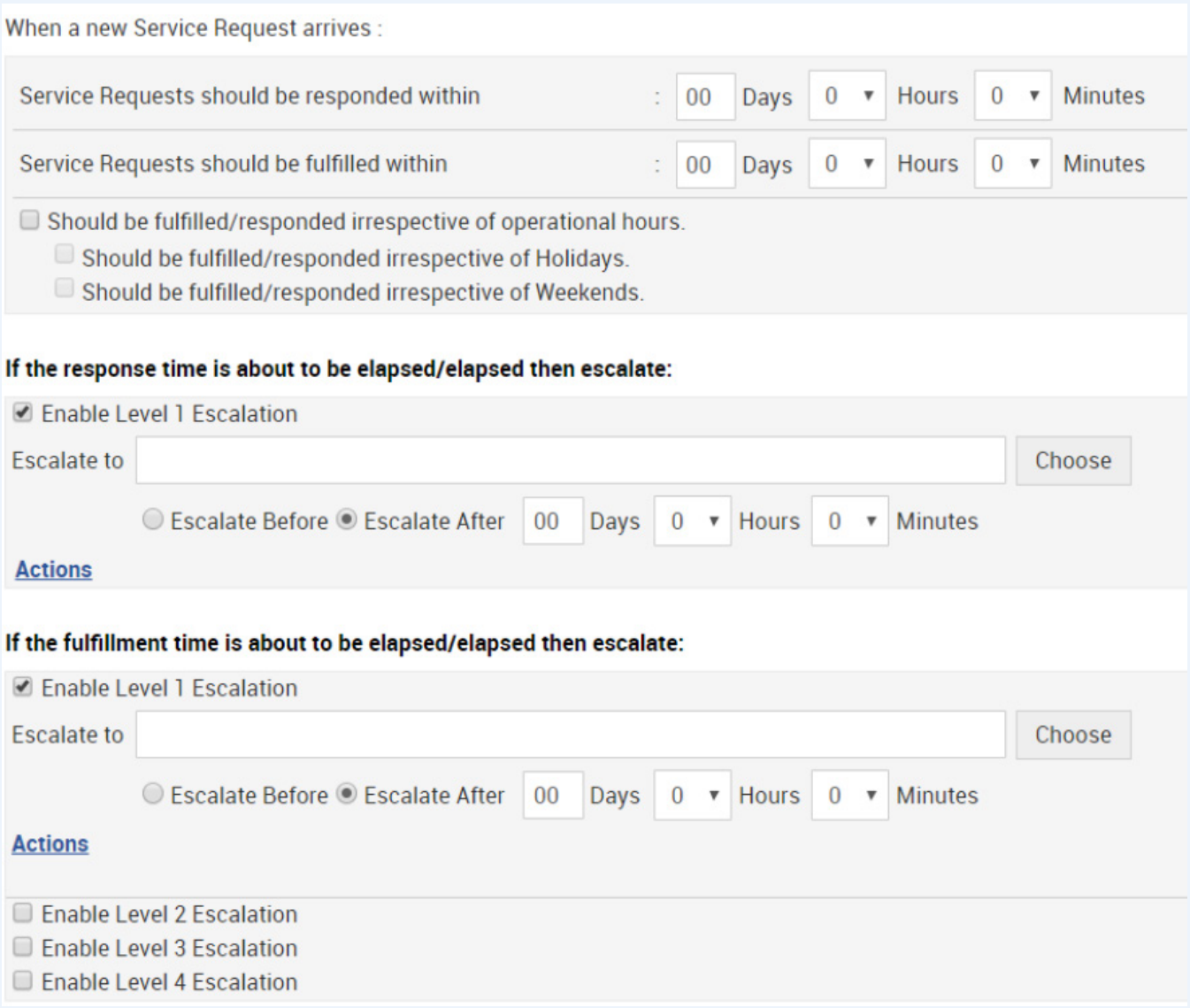
### ManageEngine product(s) that can help in implementing these processes:

### ServiceDesk Plus and Analytics Plus

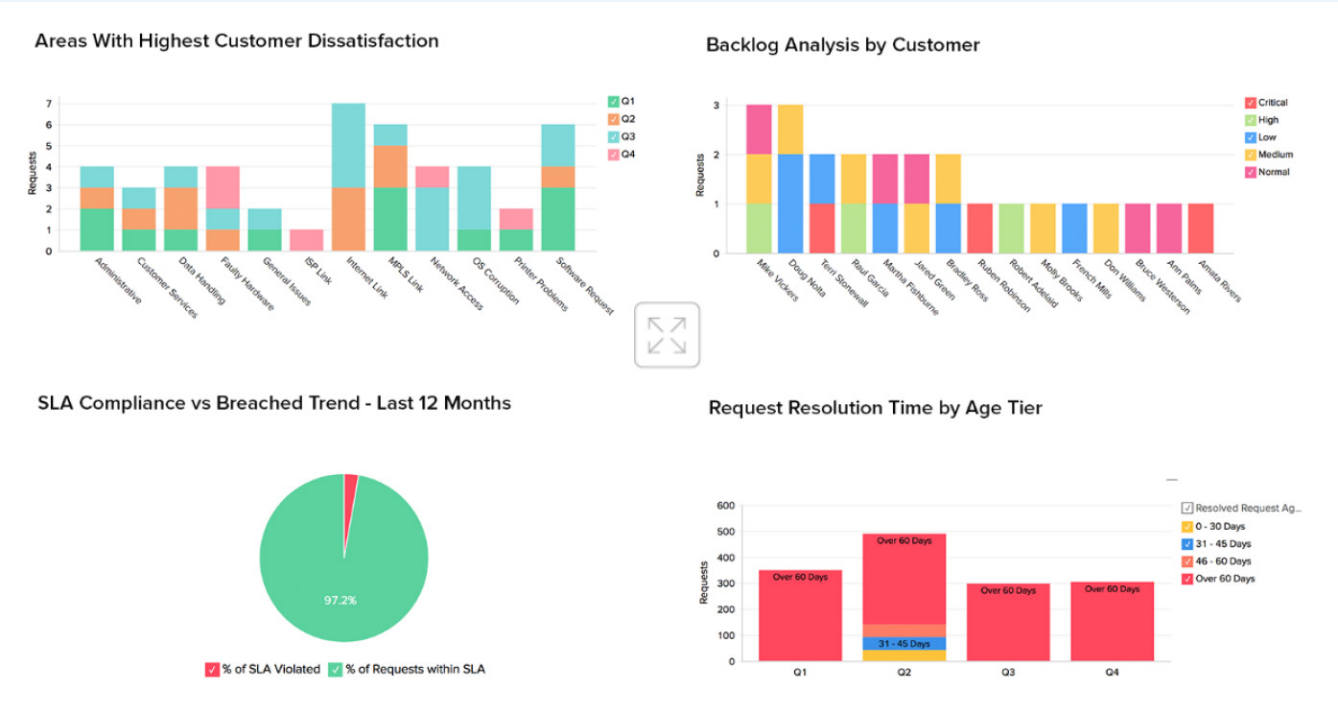
- The services agreed to be delivered can be exhibited and maintained with the help of the service catalog module. The incident and service request SLA(s) for response/resolution/fulfillment corresponding to these services can be assigned and their effectiveness can be monitored, reviewed, and reported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




*Incident SLA: Response, resolution, and escalation*



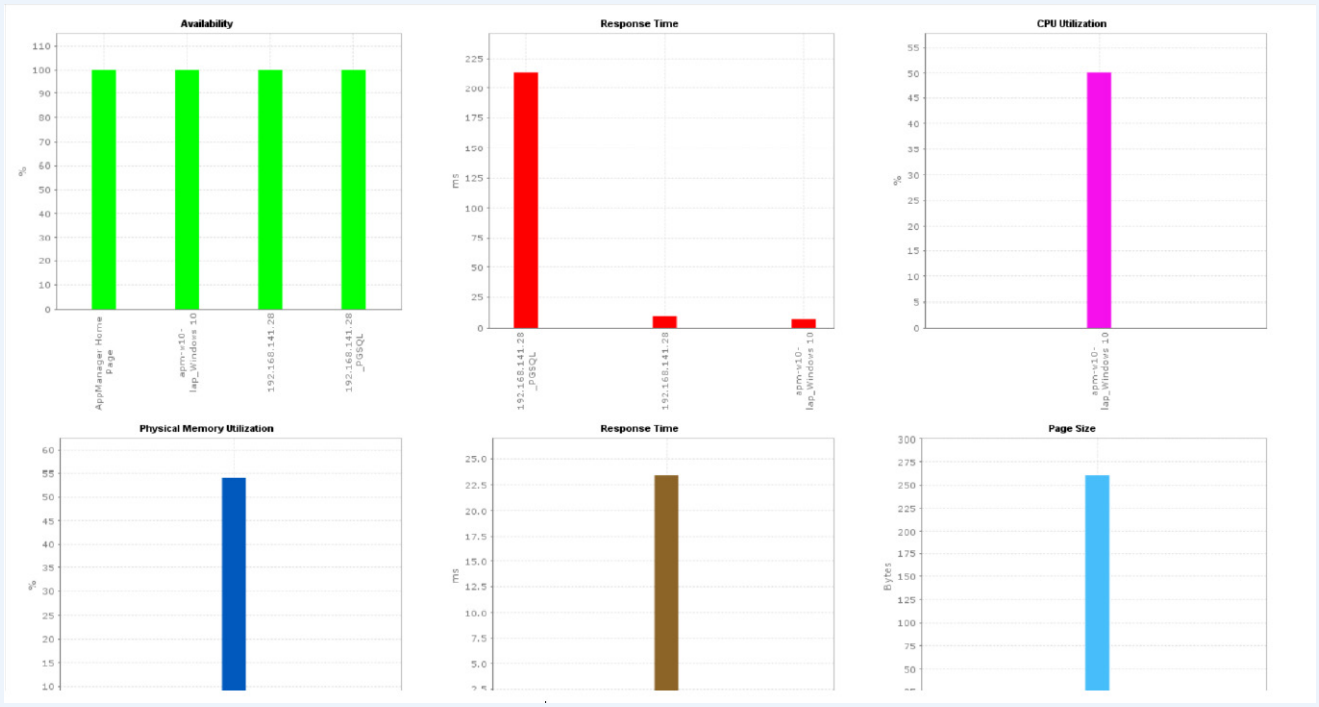

*Service request SLA: Response and fulfillment*



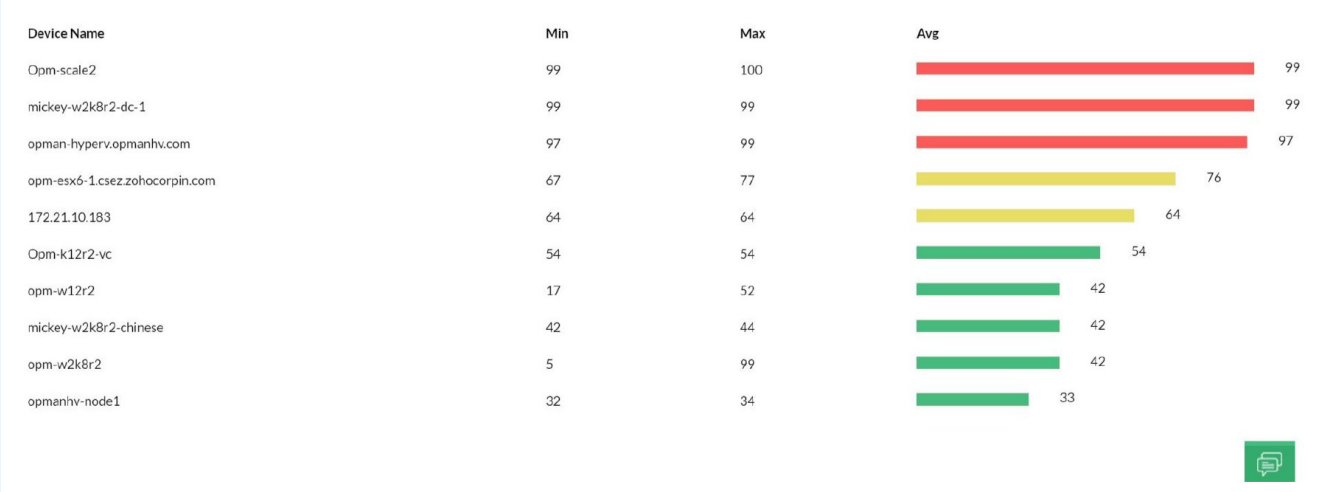

*Reporting on SLA targets (incident and service request)*

## OpManager Plus and Applications Manager

- OpManager Plus and Applications Manager together can monitor all the service components like network devices, servers, virtualization, applications, databases, websites, etc. to measure availability and performance against the service target.




*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 dashboard*

## 8.3.4 Supplier management

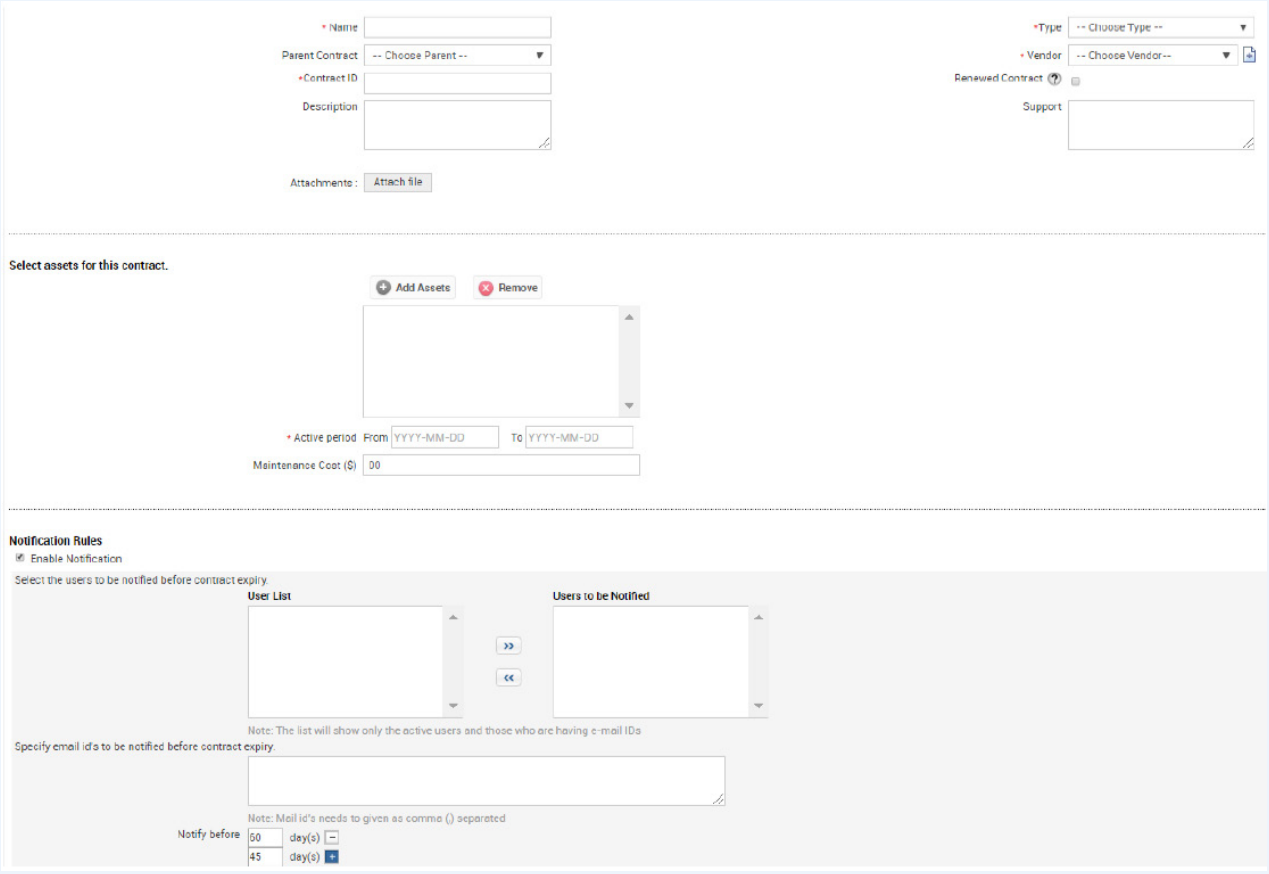
### Addressed process requirement(s):

- 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:

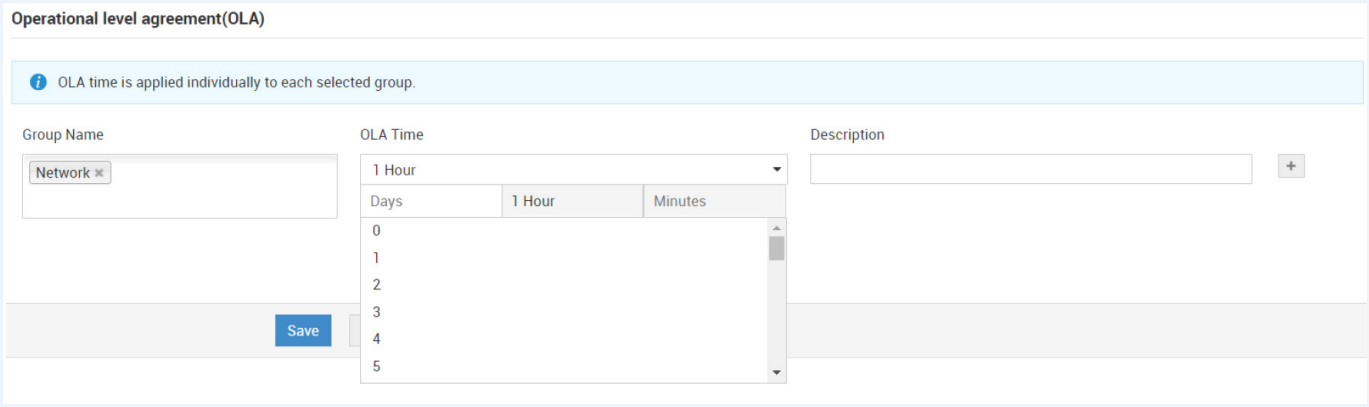
### ServiceDesk Plus

- 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.




*OLA for Internal Suppliers*

# 8.4 Supply and demand

## 8.4.1 Budgeting and accounting for services

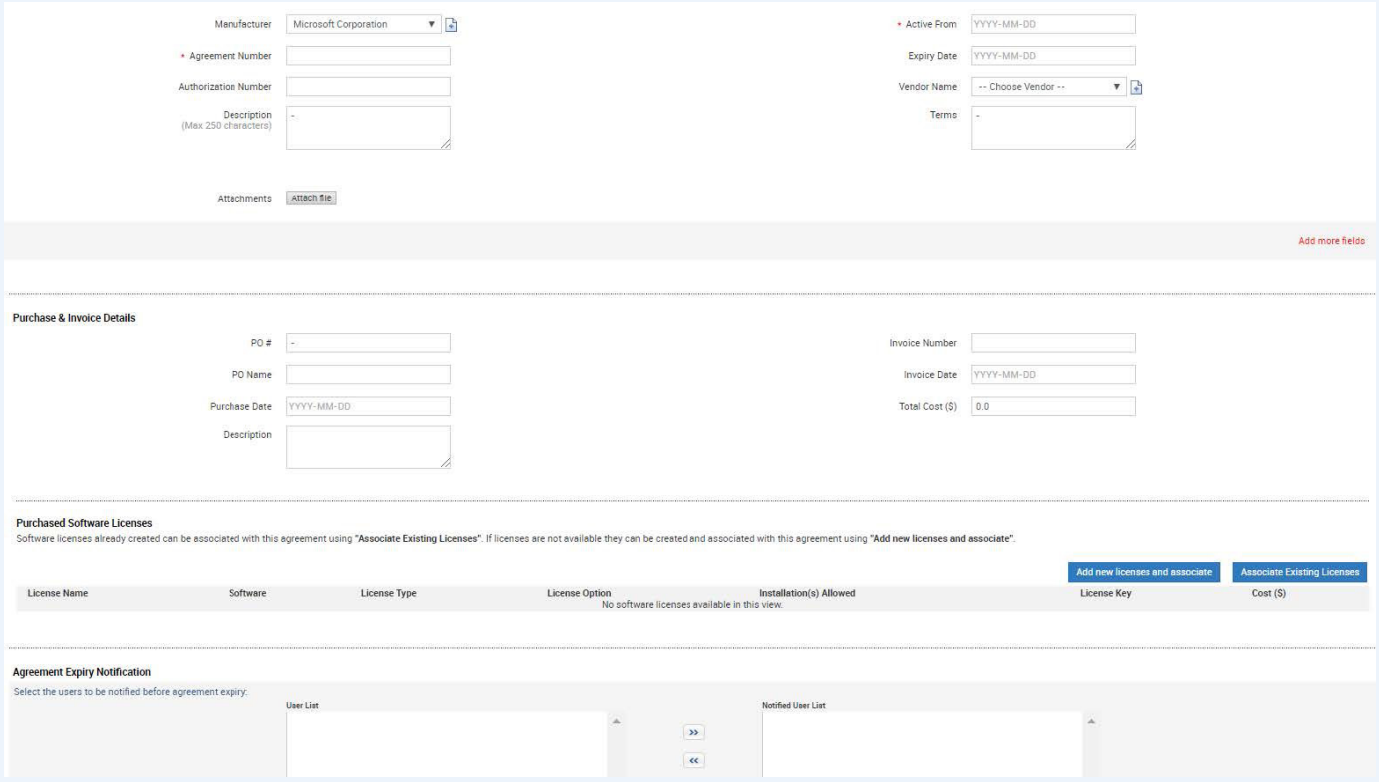
### Addressed process requirement(s):

- 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 processes:

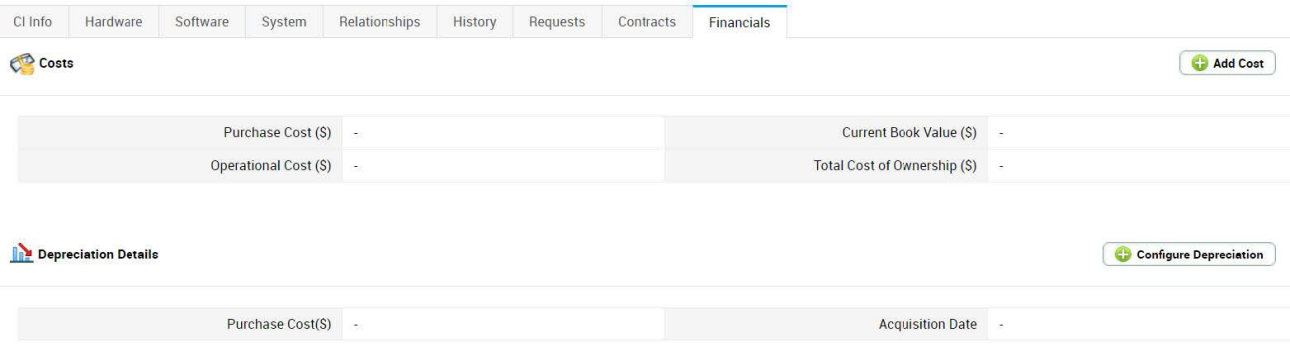
#### ServiceDesk Plus and Analytics Plus

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

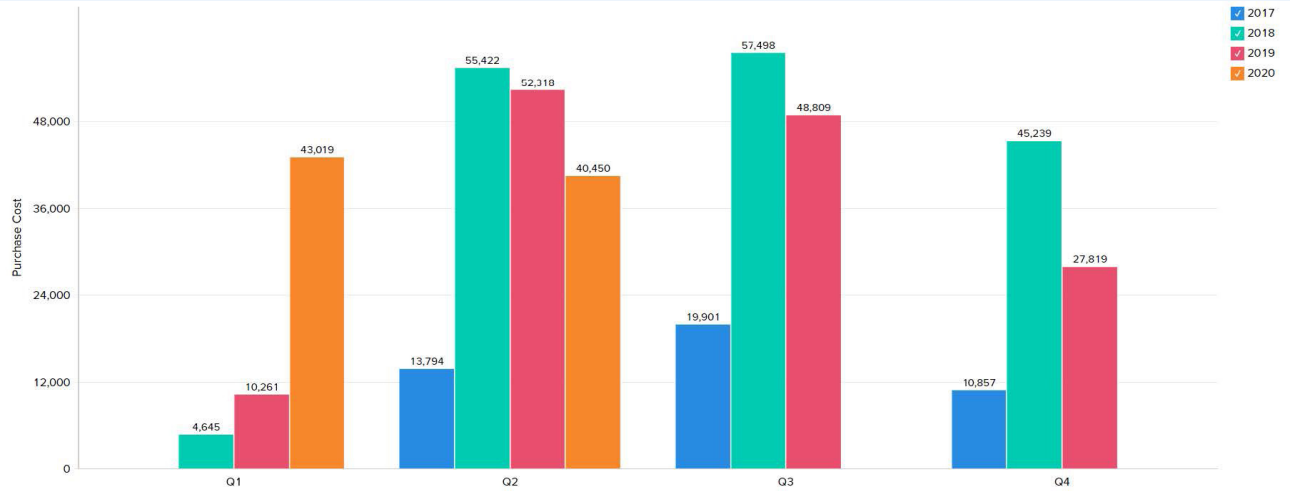



*Software license agreement*

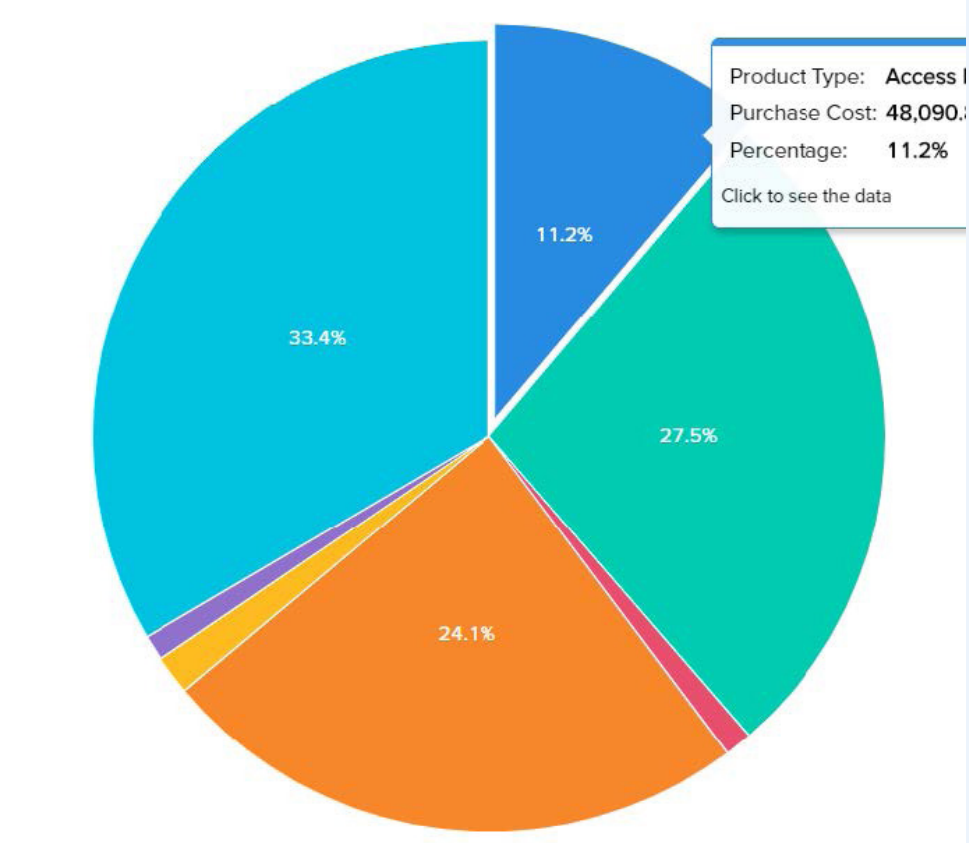
- Record and report on the actual costs and budget based on depreciation and spending. ServiceDesk Plus, when integrated with Analytics Plus, provides more visibility on the budget.



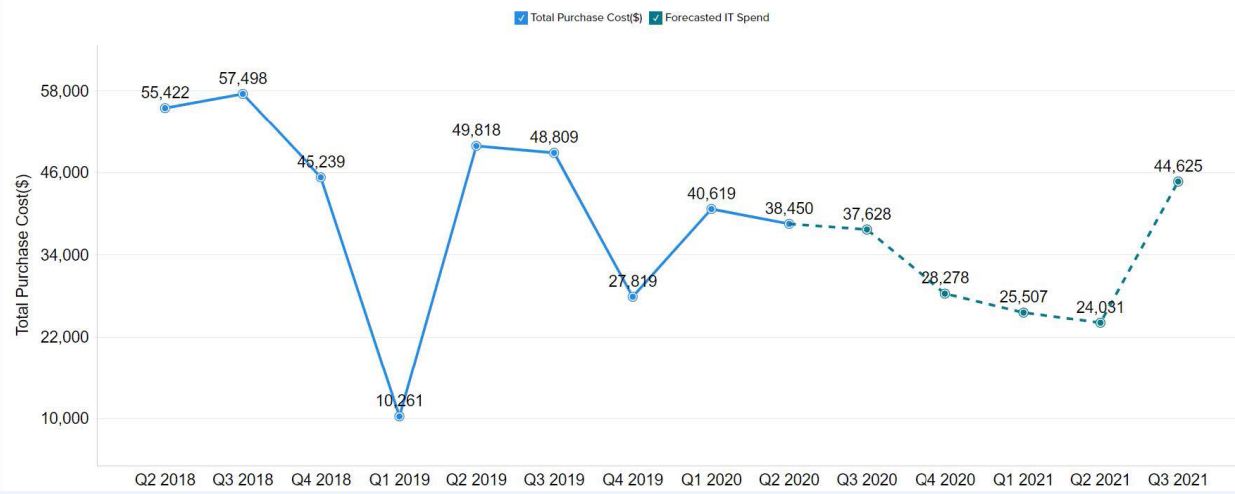

*Asset financial and depreciation details*




*Year-over-year (YOY) comparison of IT spending based on purchase costs*




*IT spending*




*IT spending forecast*

## 8.4.2 Demand management

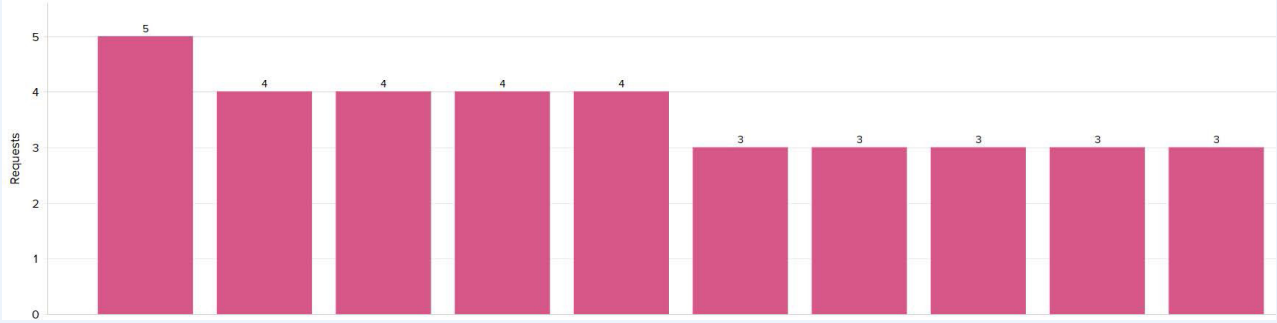
### Addressed process requirement(s):

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

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

### 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.

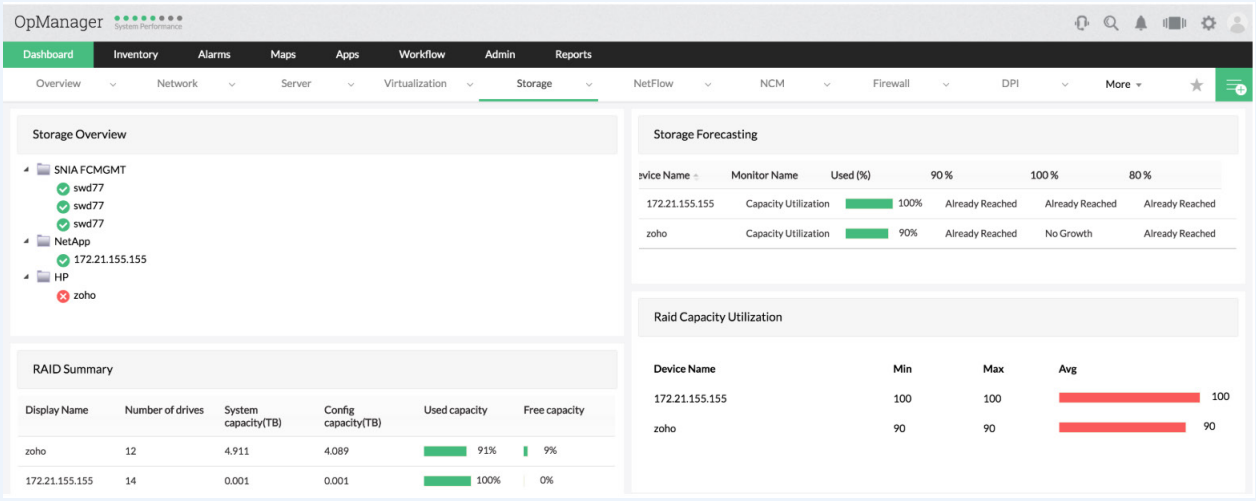



*Top 10 frequently requested service*

### OpManager Plus and Applications Manager

- 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

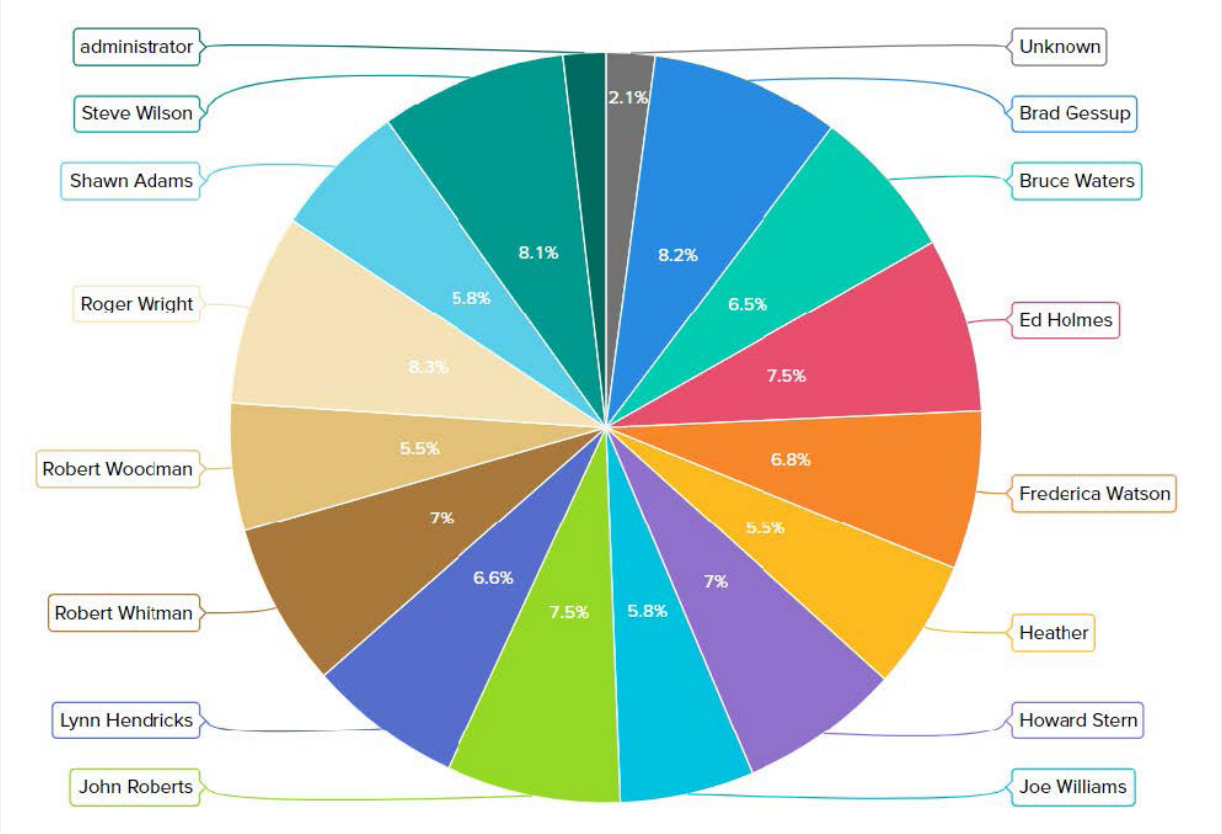
### Addressed process requirement(s):

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

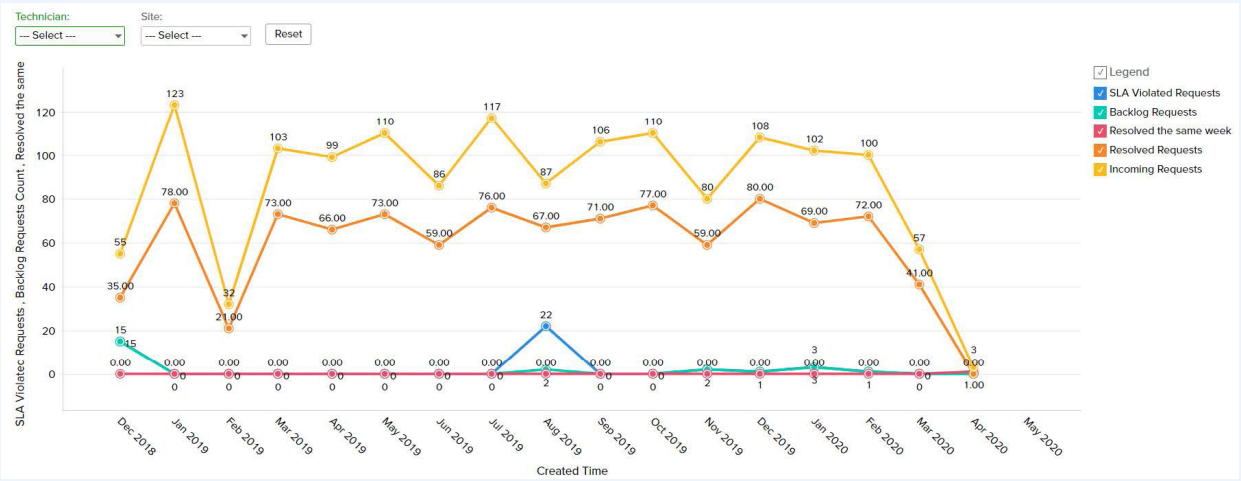
### ManageEngine product(s) that can help in implementing this process:

### 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. by integrating with Analytics Plus.



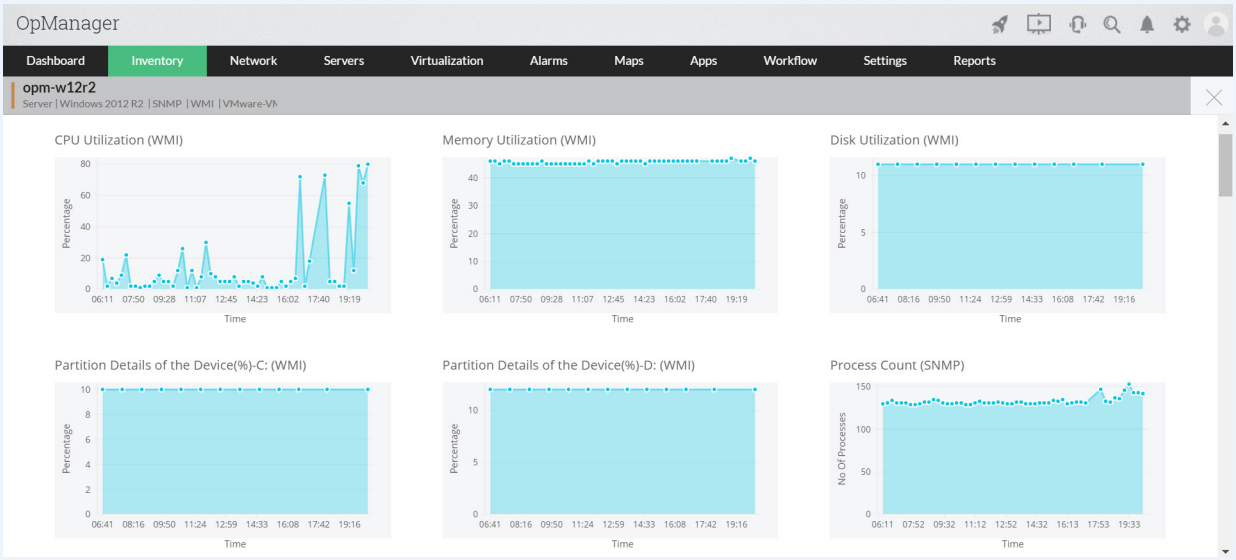

*Technician load: Open requests*



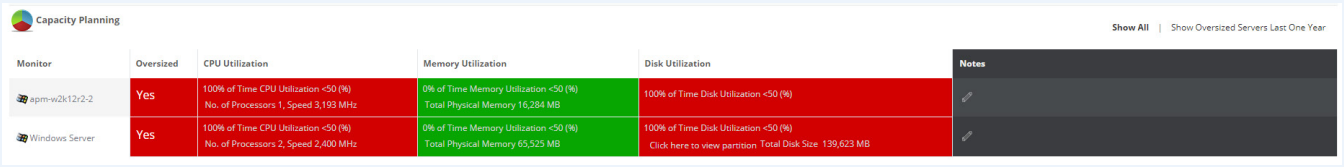

*Incoming, resolved, backlogged, and same-week resolution service requests*

## OpManager Plus and Applications Manager

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




*Server performance monitoring*

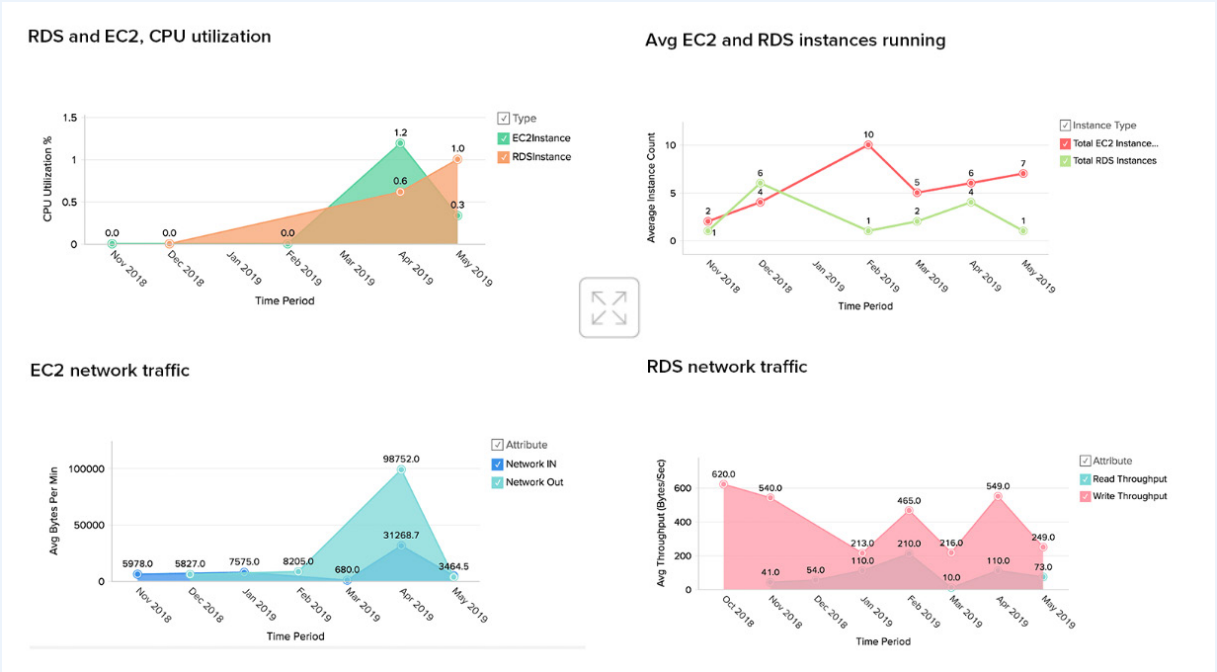



*Report on over-sized servers*

## 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

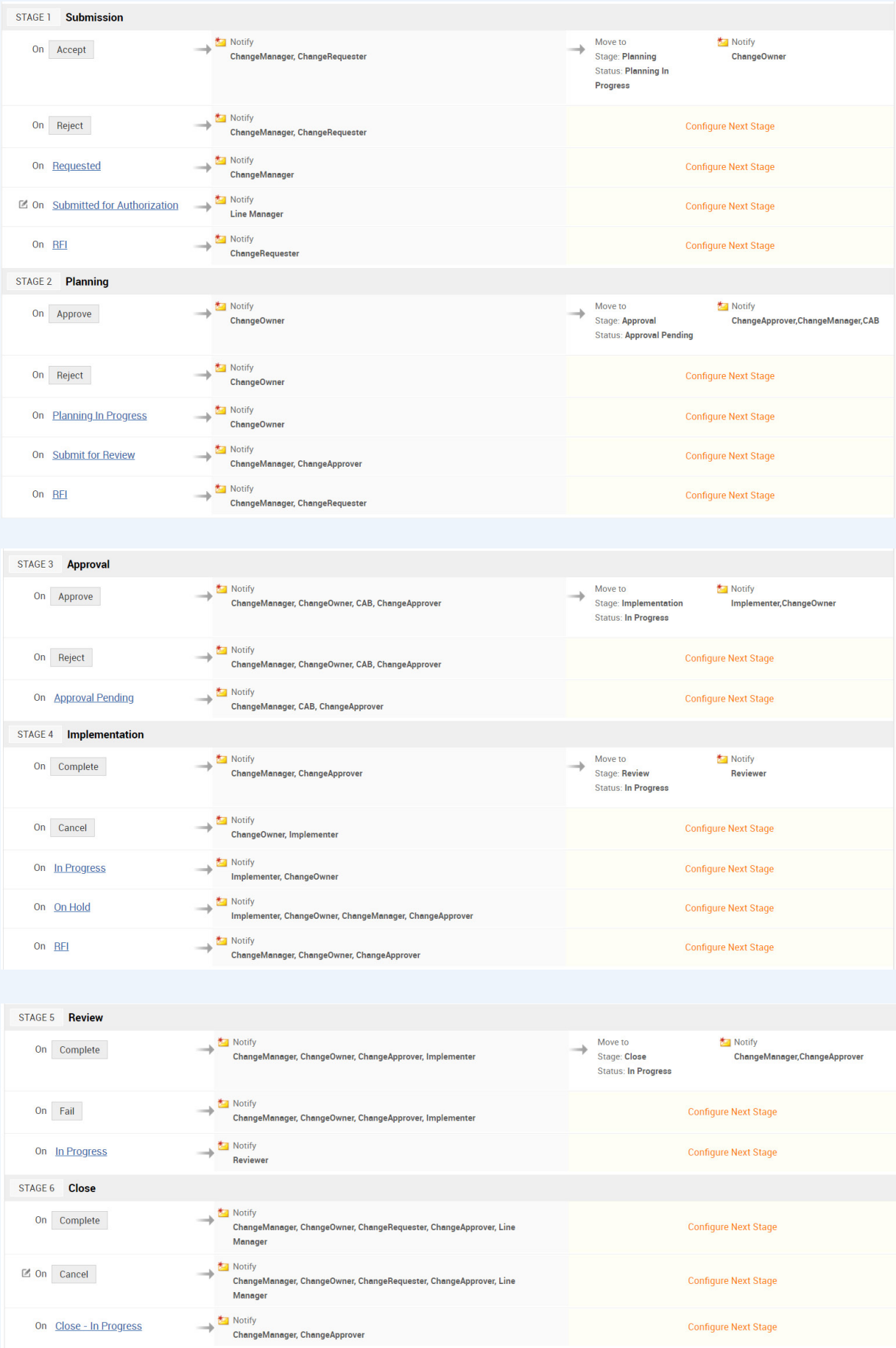
### Addressed process requirement(s):

- 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.

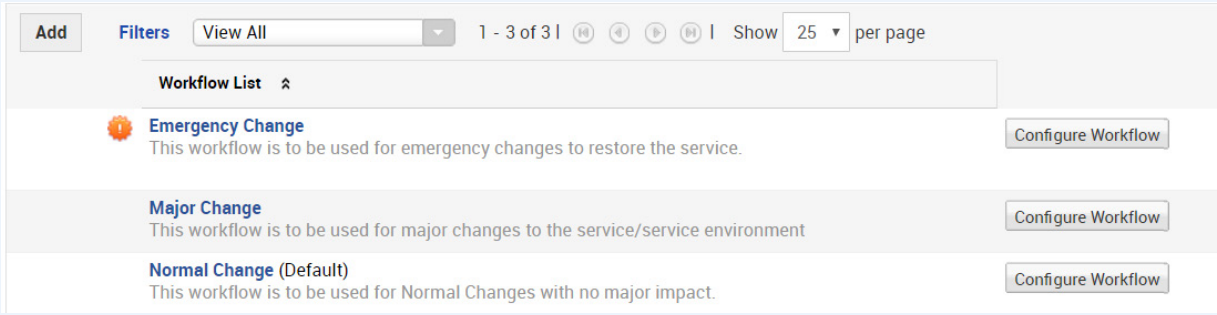
### ManageEngine products that can help in implementing these processes:

**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.

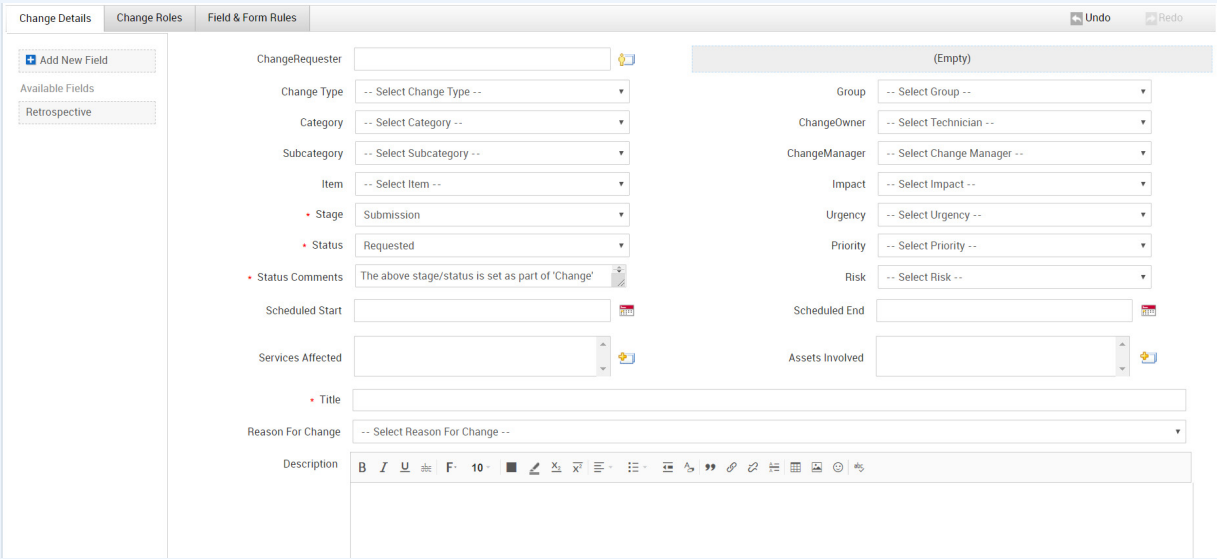



*Configurable change workflow*

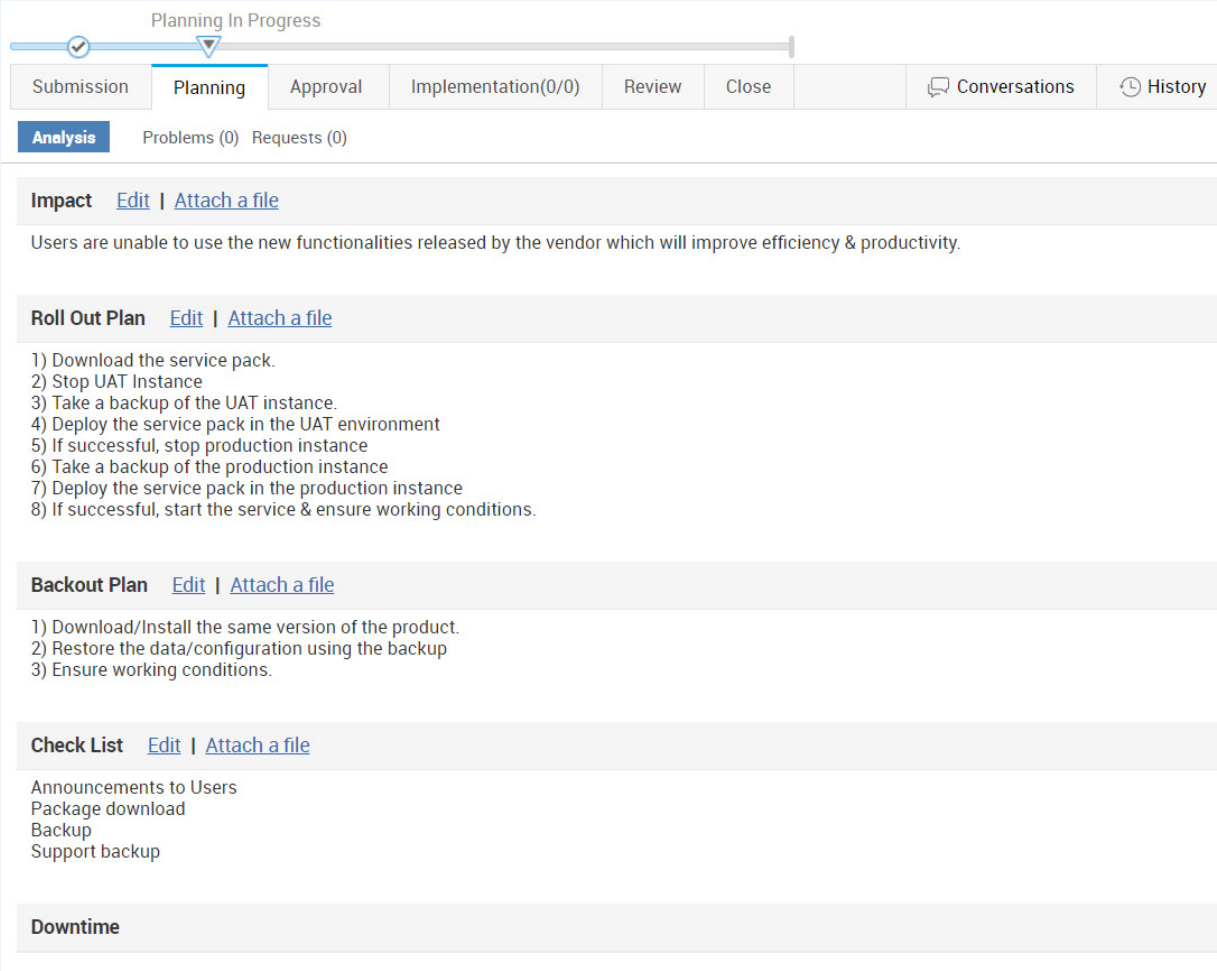



*Multiple change workflows*

- 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.

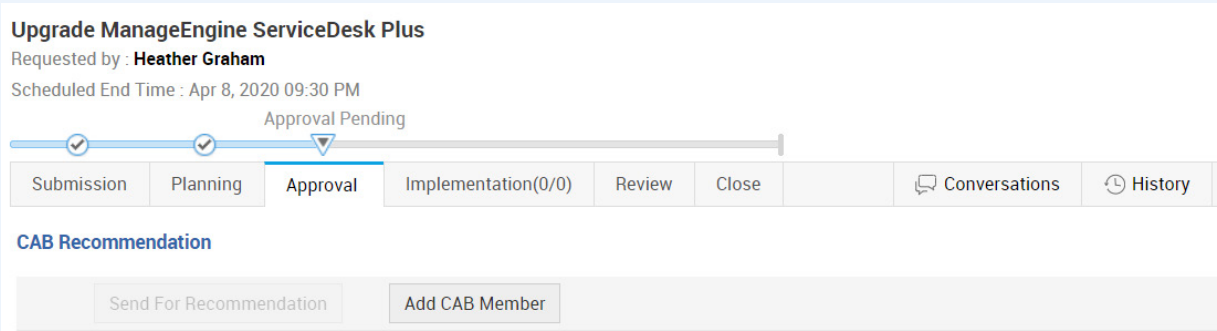



*Configurable RFC template*



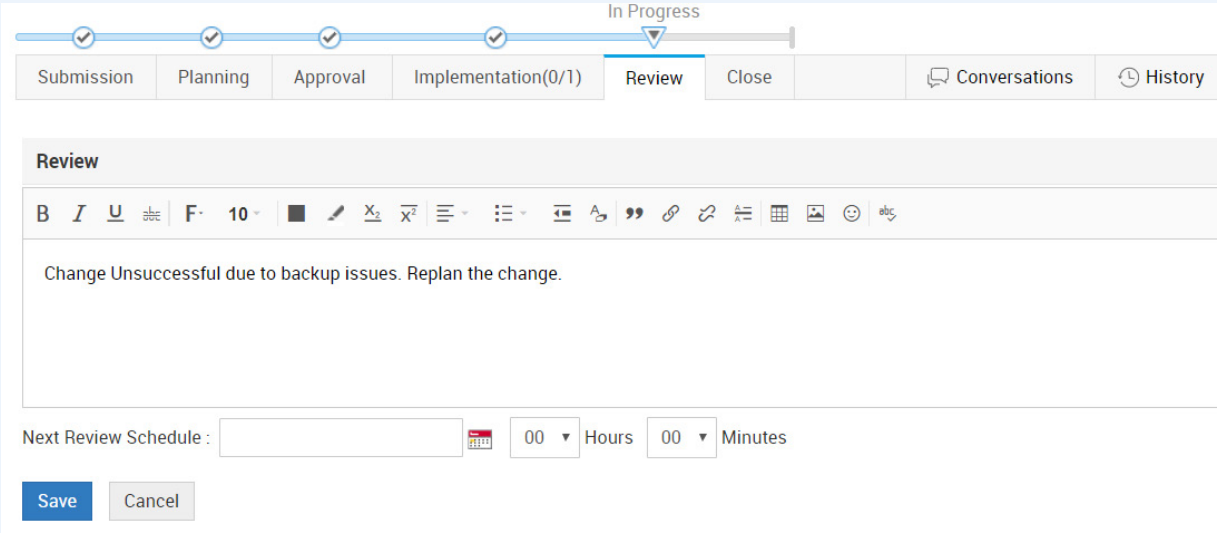

*Change planning*

- 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, the details can be communicated to interested parties through notifications.




*Change approval*

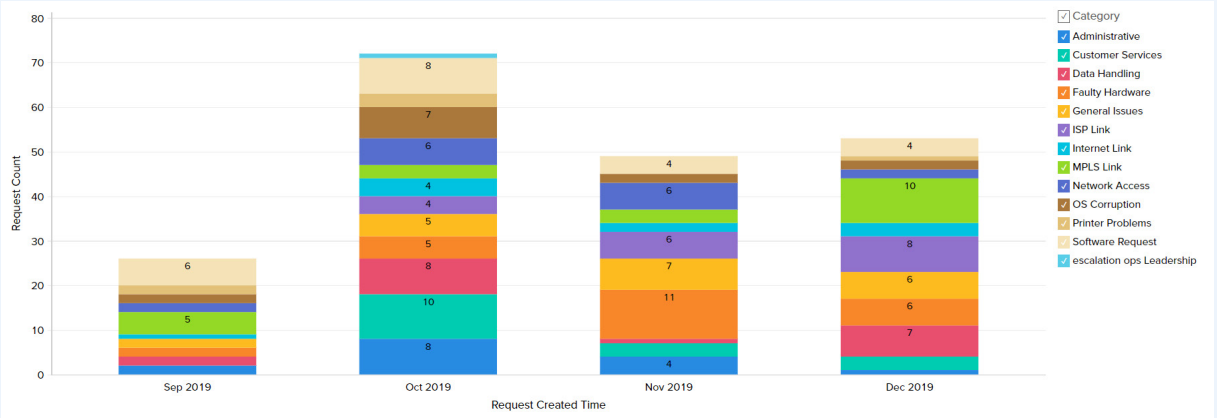
- Unsuccessful change requests will follow the configured workflow, like returning to previous stages or closing the change record.



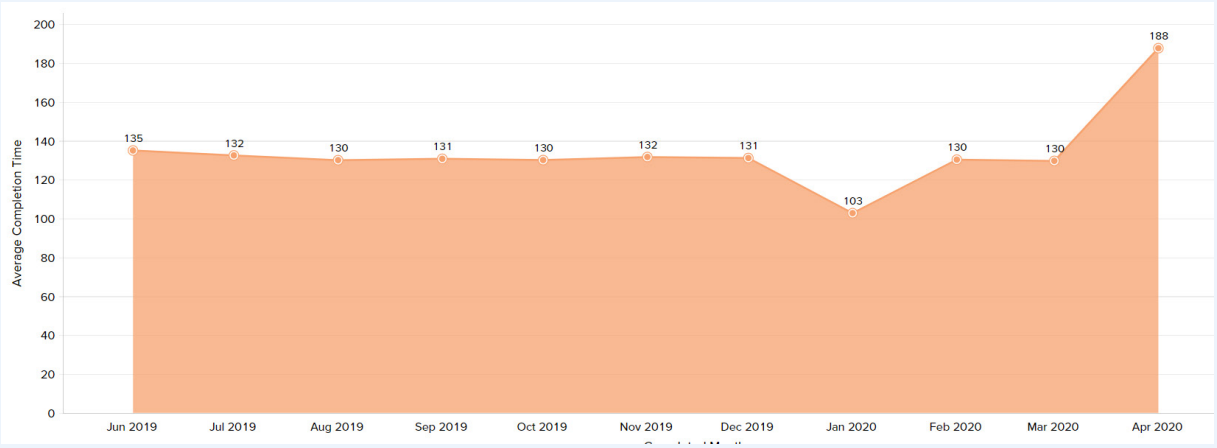

*Change review*

## 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 effective-ness.




*Trend requests for analyzing changes*




*Average change completion time (in days)*

## 8.5.2 Service design and transition

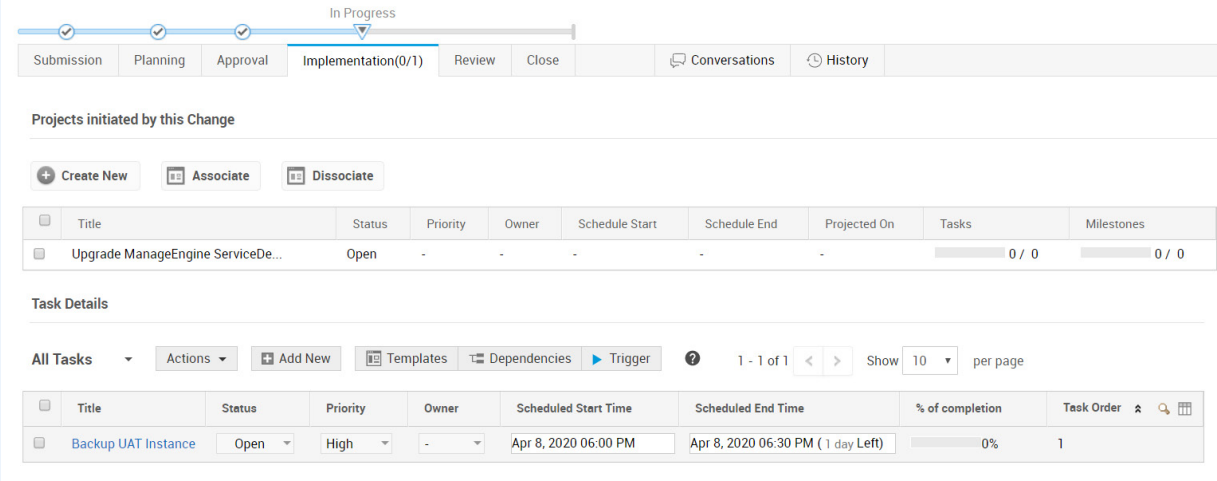
### Addressed process requirement(s):

- 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.

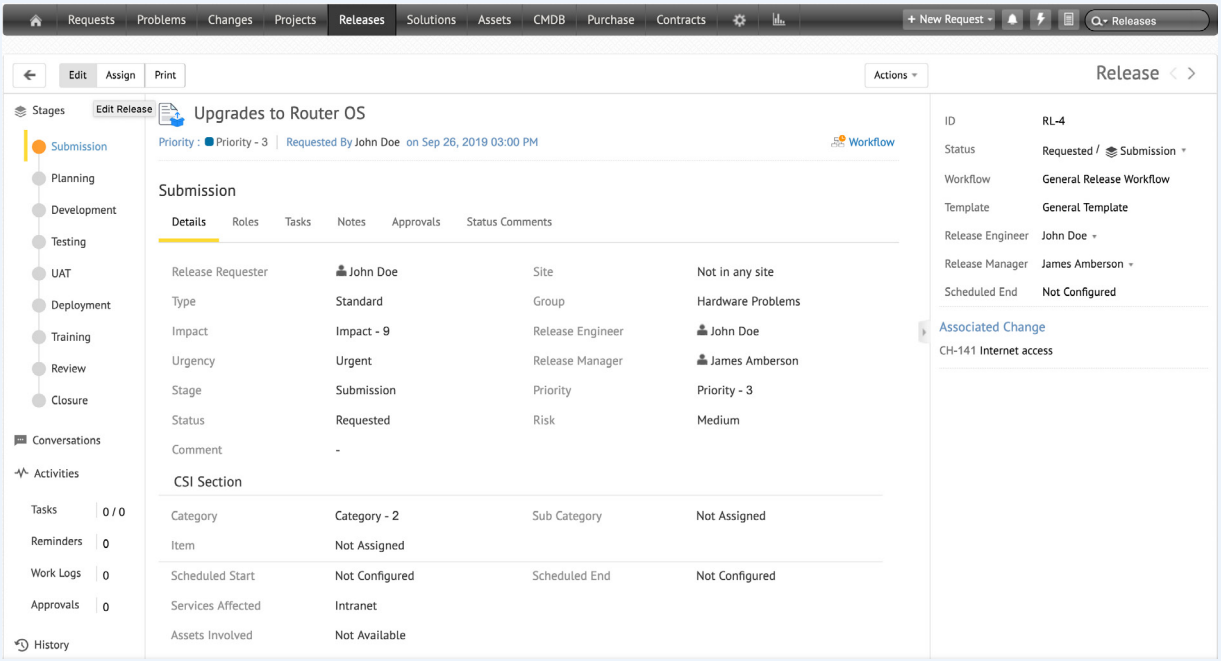
### ManageEngine product(s) that can help in implementing these processes:

**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 (available in both on-premises and on-cloud versions), and release (available only in cloud version) modules.




*Implementation: Projects and tasks*




*Release management*

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

## 8.5.3 Release and deployment management

### Addressed process requirement(s):

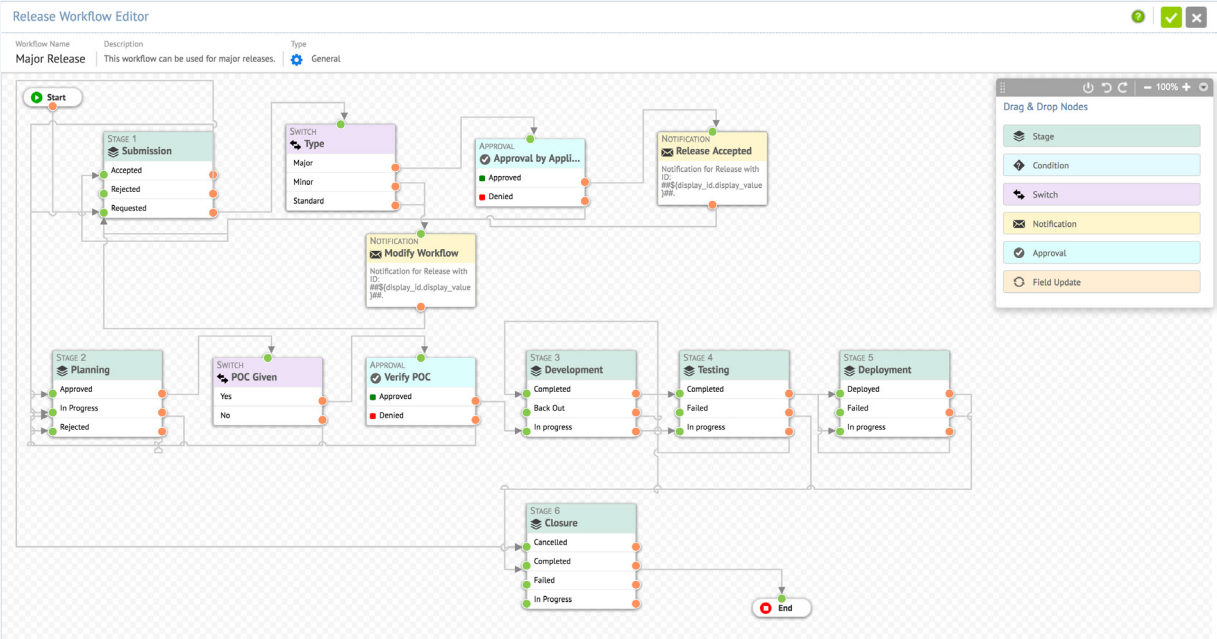
- The types of release, including emergency release, their frequency, and how they are to be managed, shall be defined.
- The deployment of new or changed services and service components into the live environment shall be planned and coordinated with change management and include references to the related 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 incidents related to a release post deployment, for opportunities for improvement.

### ManageEngine products that can help in implementing these processes:

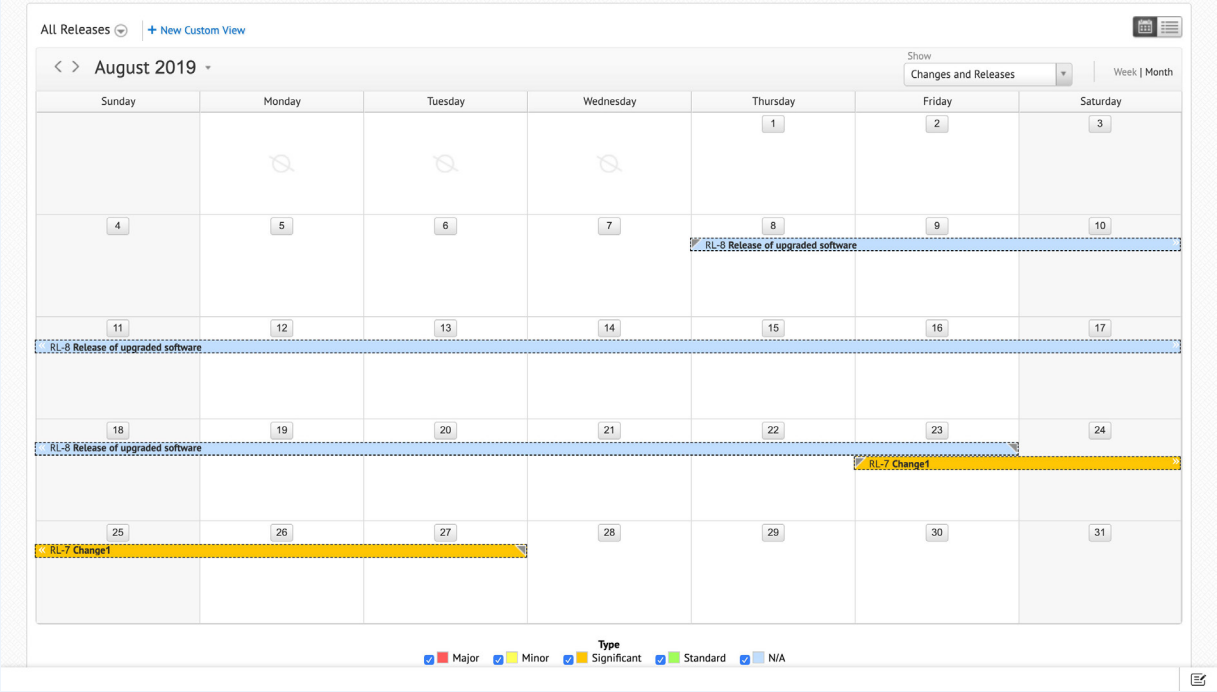
**ServiceDesk Plus**

- 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 supports approvals as required in different stages.

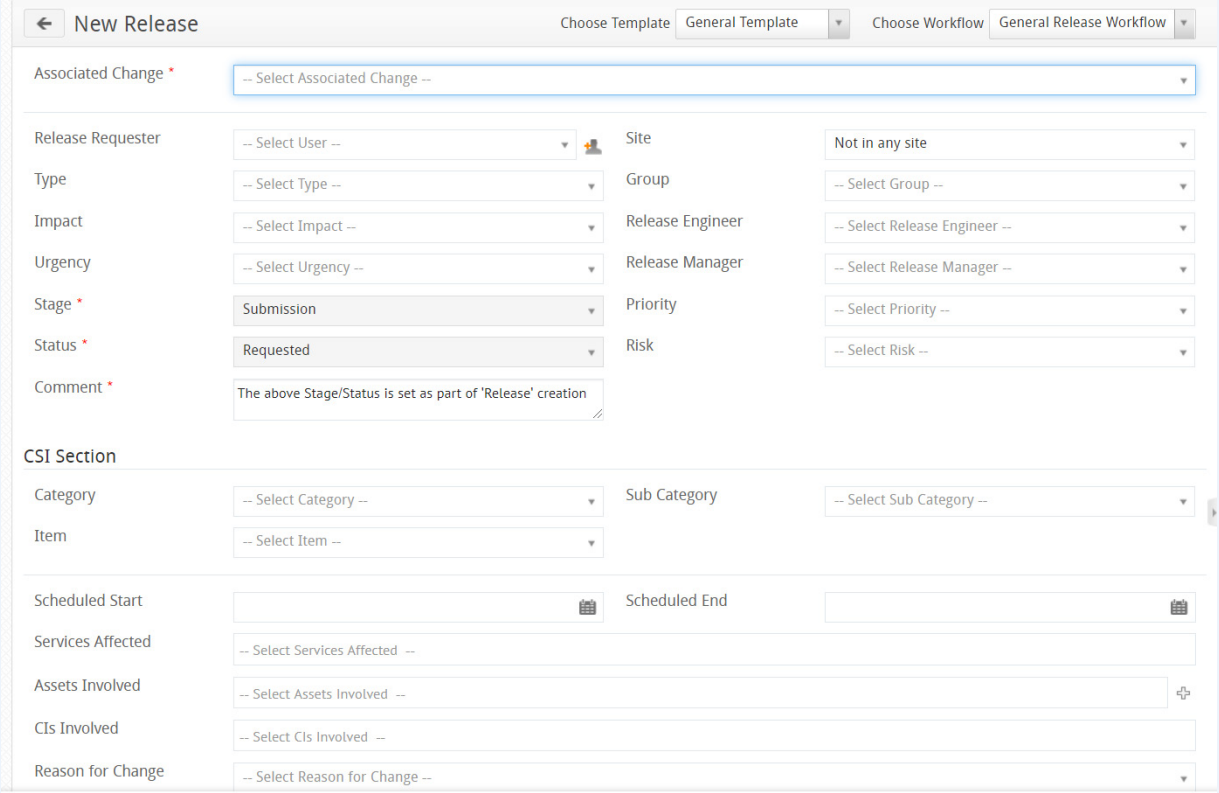



*Release workflow*



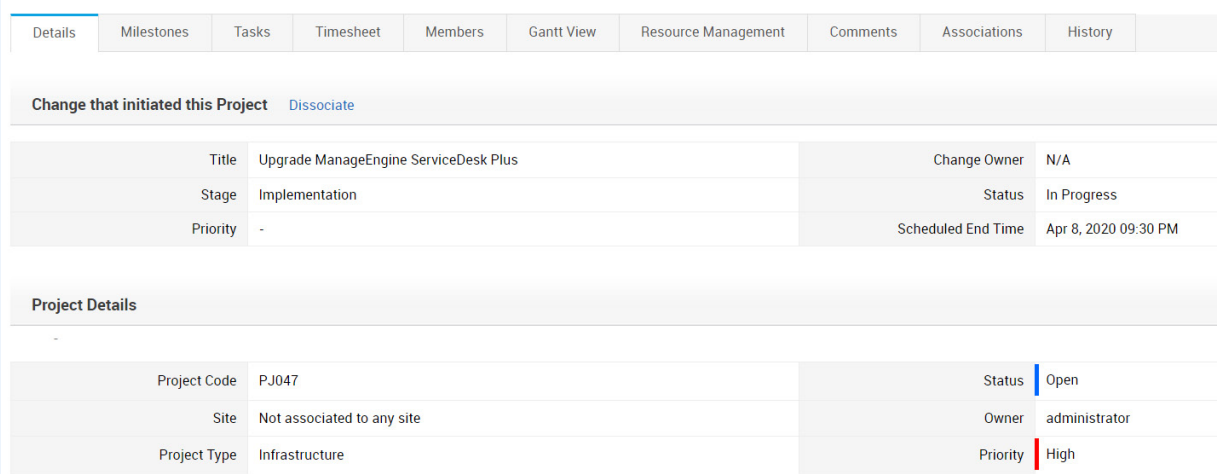

*Release calendar*

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




*New release template: Change association*

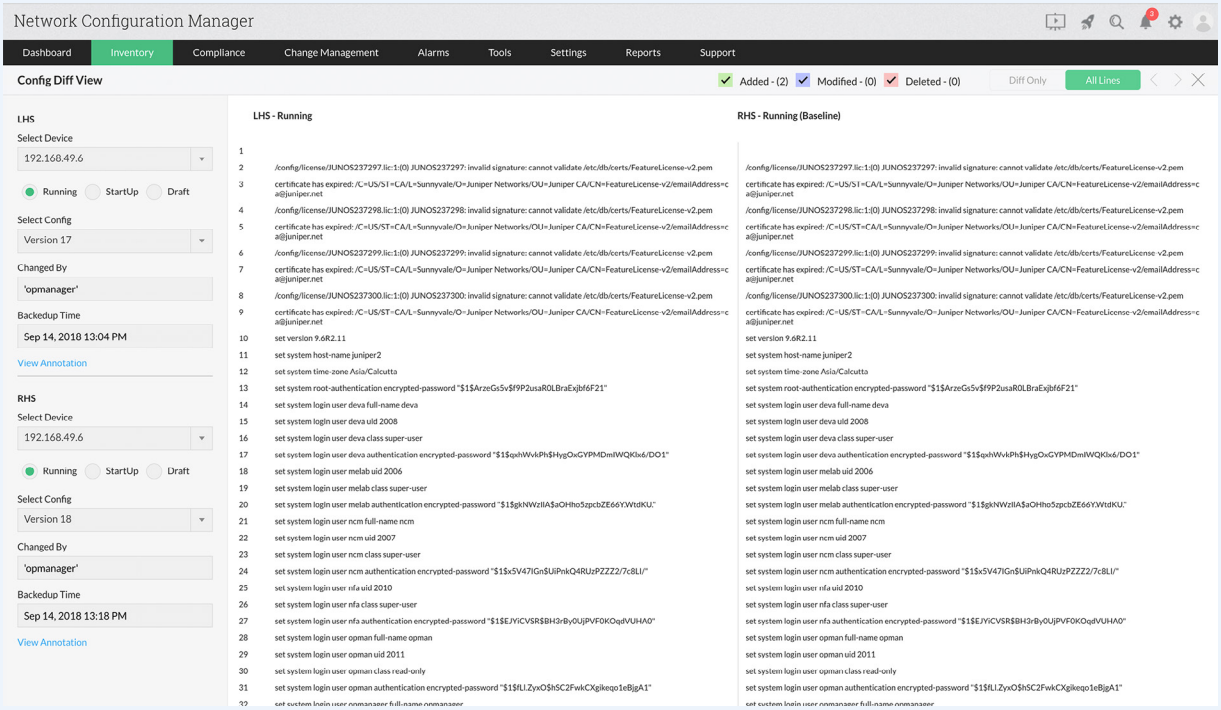
- Reporting module helps you to analyze the effectiveness of the release to identify opportunities for improvement.
- For the on-premises version, the same can be handled using a combination of the change and project modules.




*Project management: Change association*

## OpManager Plus

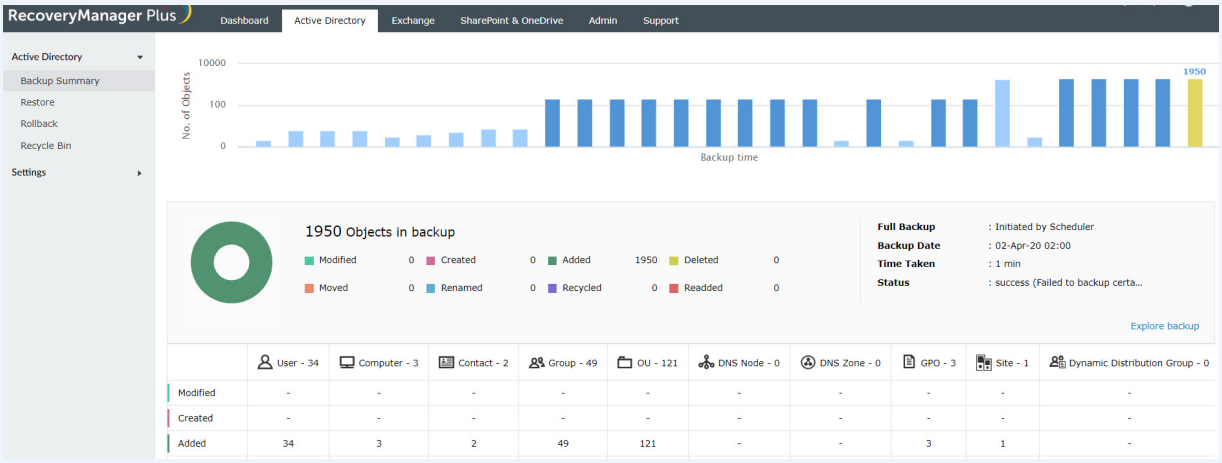
- OpManager's Network Configuration Manager component can take a back-up of the network device configurations as a baseline before deployment of a release, compare the changes, and rollback changes as required.




*Compare configurations*

## AD360

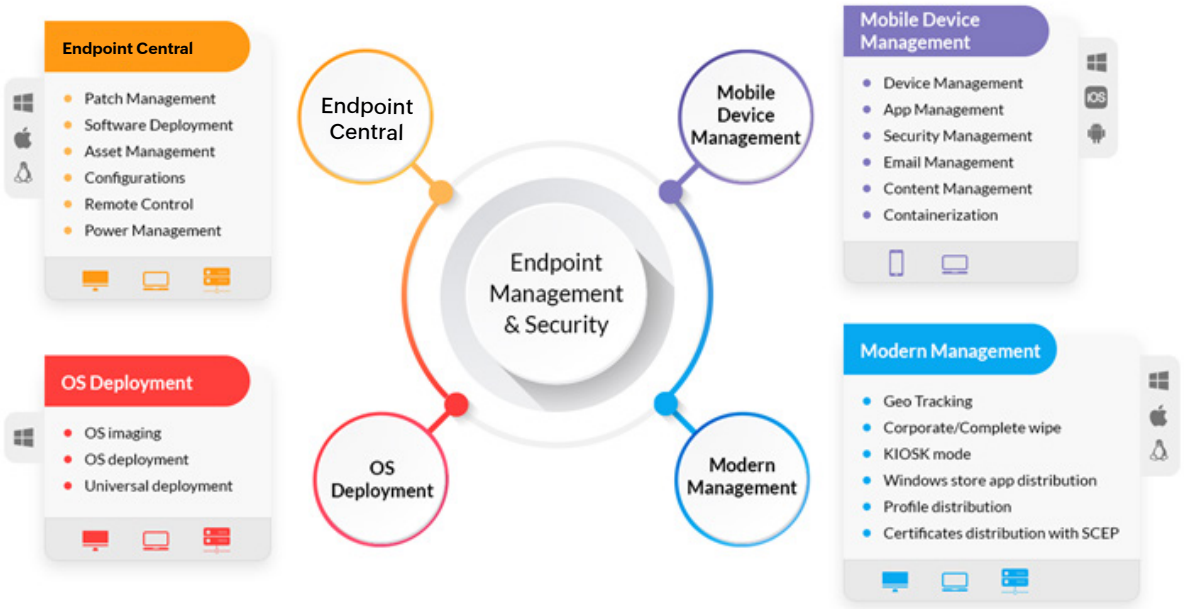
- The Recovery Manager Plus component of AD360 can backup AD objects, Exchange mailboxes, OneDrive for Business, and SharePoint Online sites as baselines, and offers simple and granular restoration options.




*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

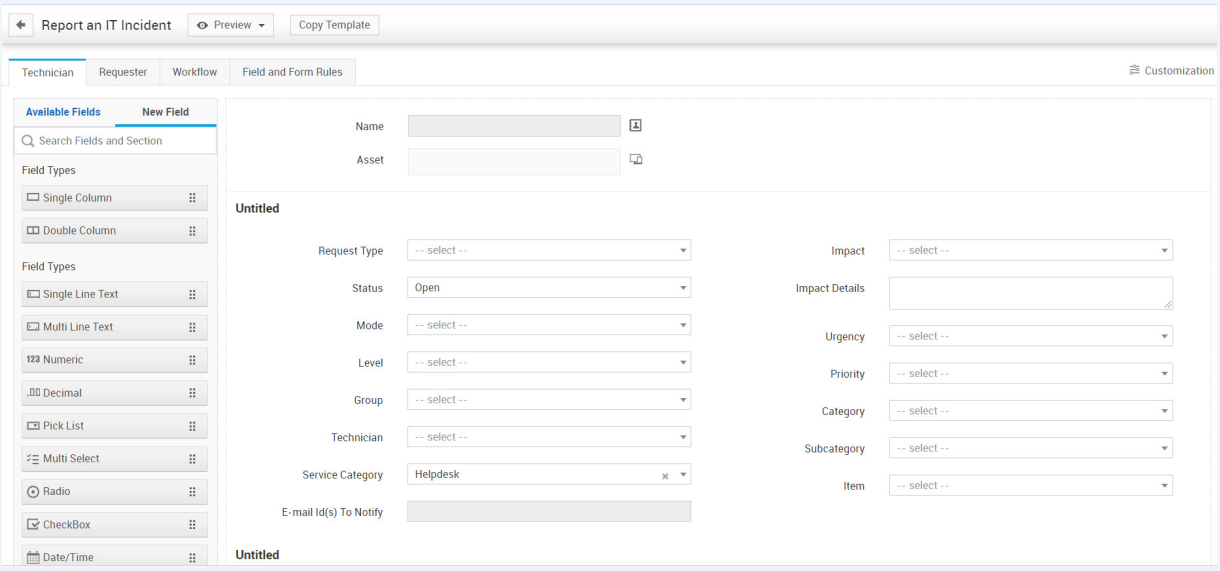
### Addressed process requirement(s):

- 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.

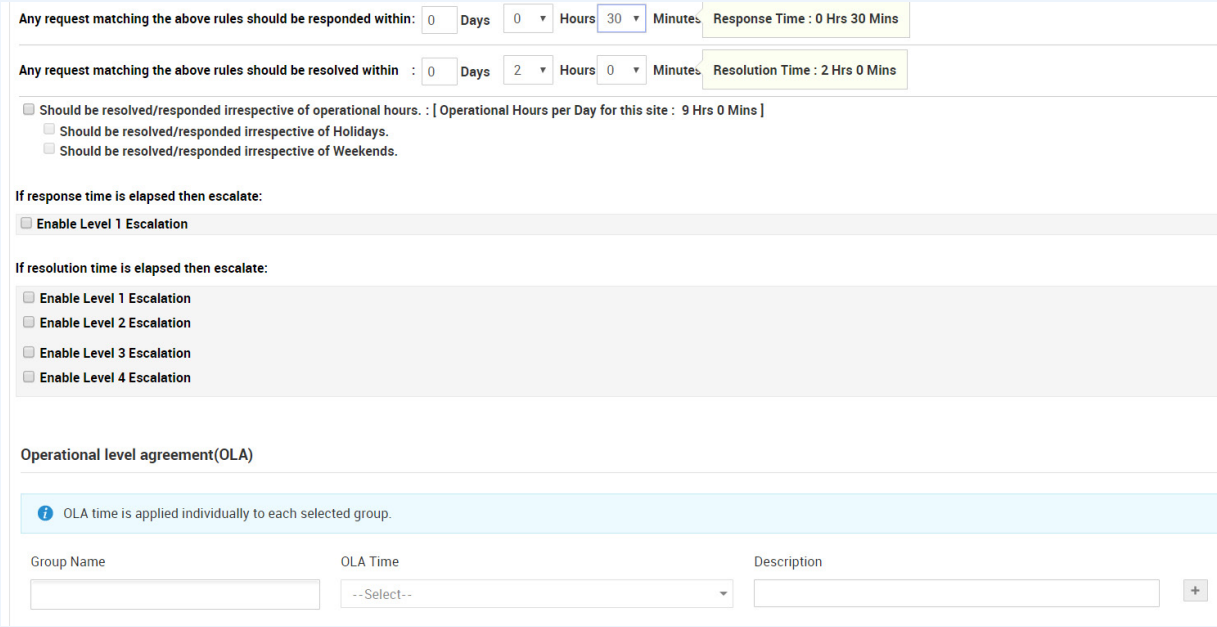
### ManageEngine product that can help in implementing these processes:

### ServiceDesk Plus and Analytics Plus

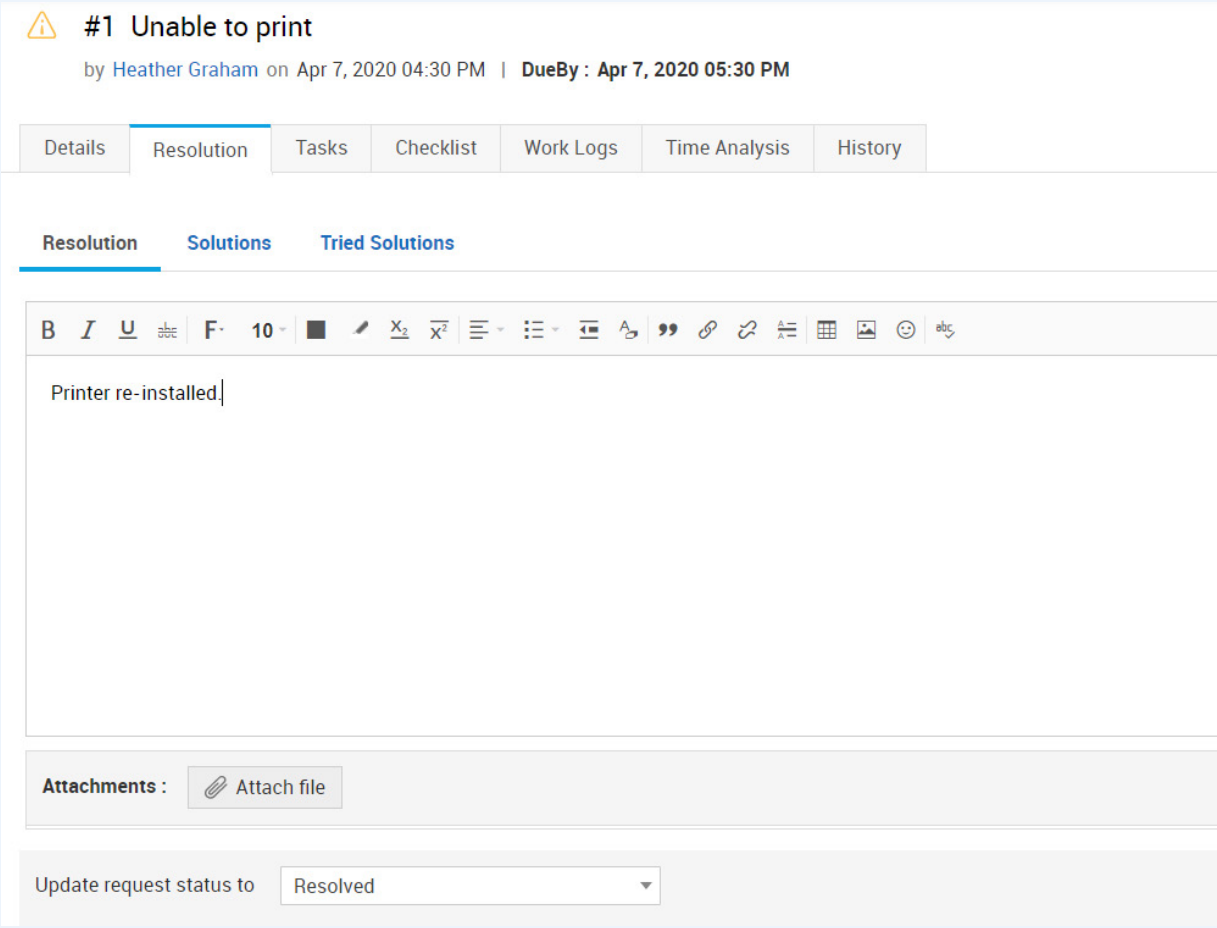
- The Incident management module helps you to record incidents using customizable templates, prioritize based on impact and urgency matrix, escalate based on response and resolution time, update actions taken, resolve, and close the incidents.




*Customizable incident template*

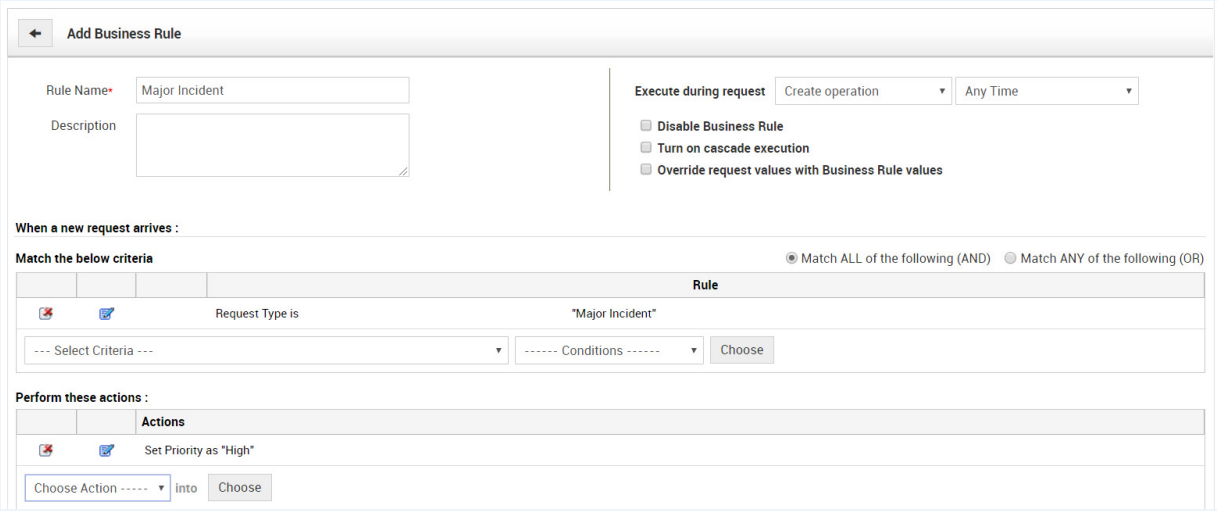



*Response, resolution, and escalation*



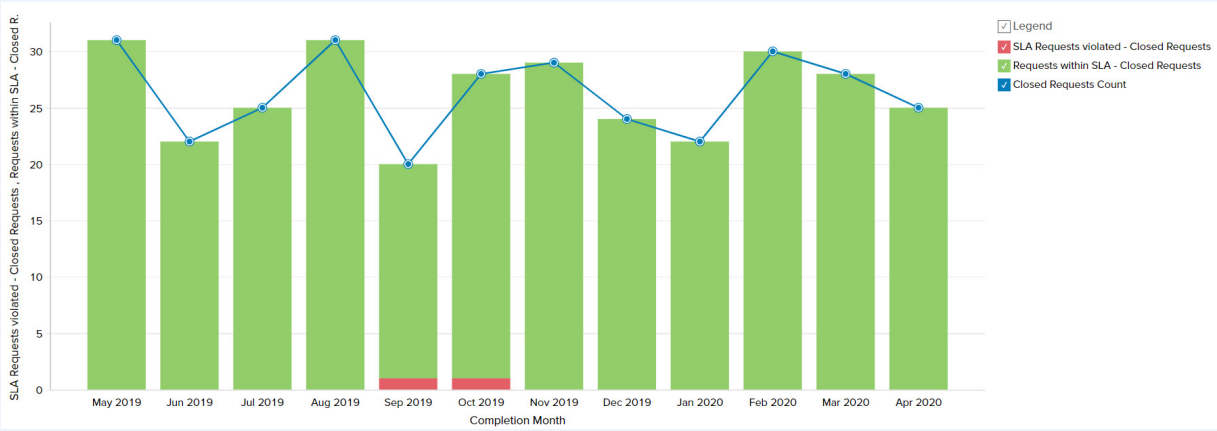

*Update actions, and resolve/close incidents*

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

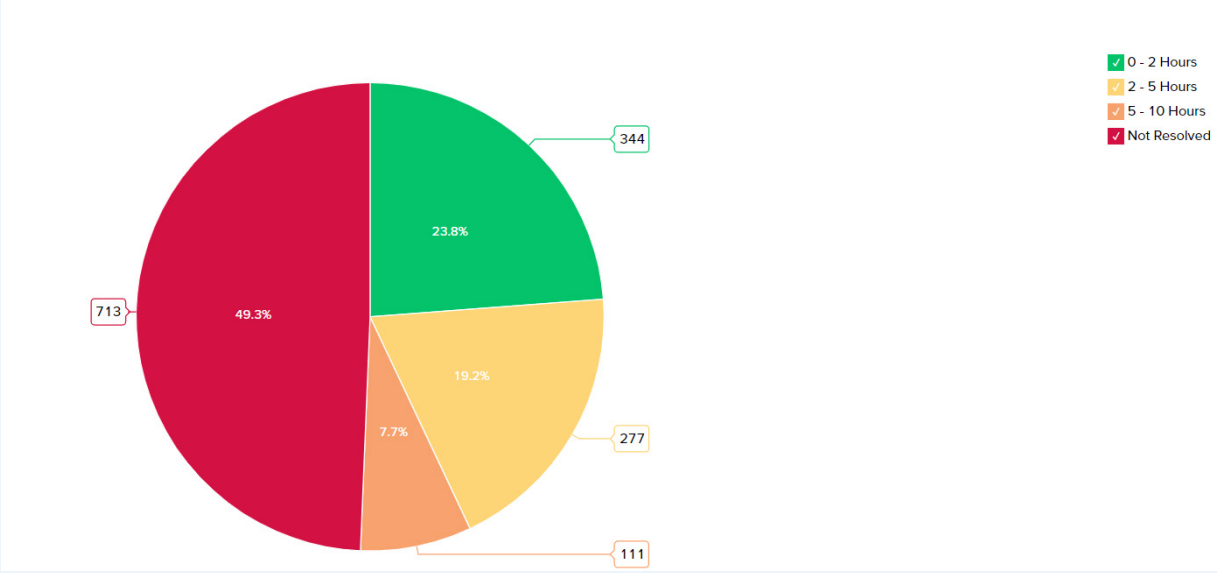



*Business rules*

- 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

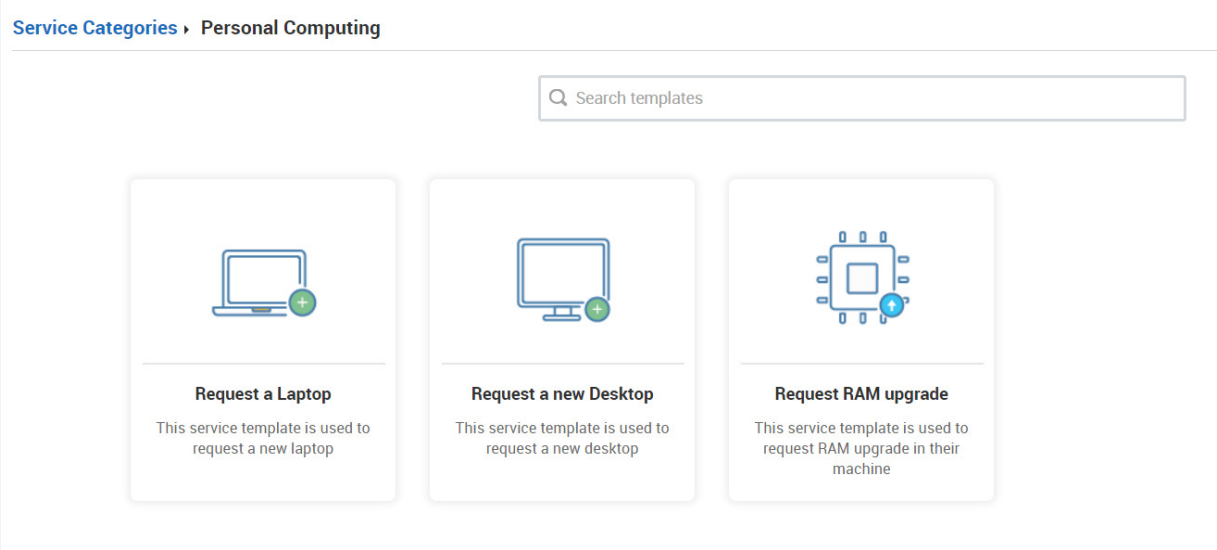
### Addressed process requirement(s):

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

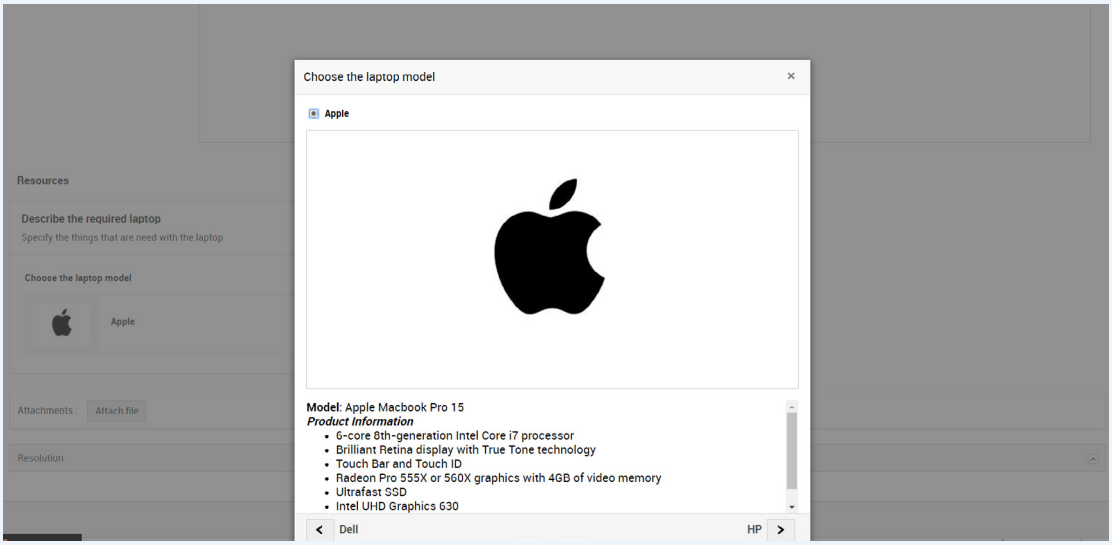
### ManageEngine product that can help in implementing these processes:

**ServiceDesk Plus**

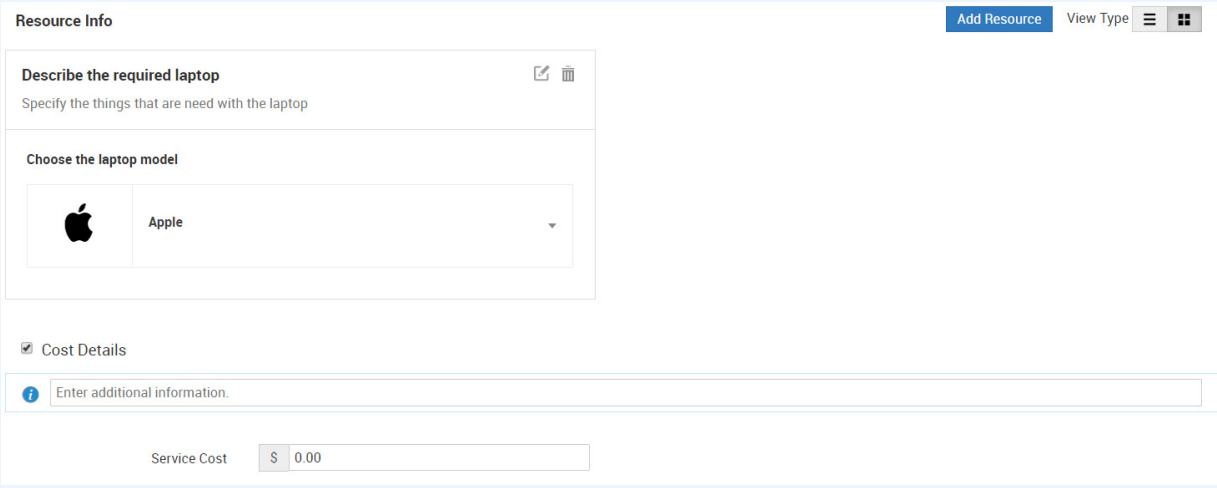
- The Service Catalog module helps you to create different service request templates under different categories, allowing users to choose the required service requests. Each template can have its own workflow process for approval, assignment, SLA, prioritization, and required fields to automate the flow of fulfillment.
- The fulfilled service requests can be updated with actions taken and then closed.



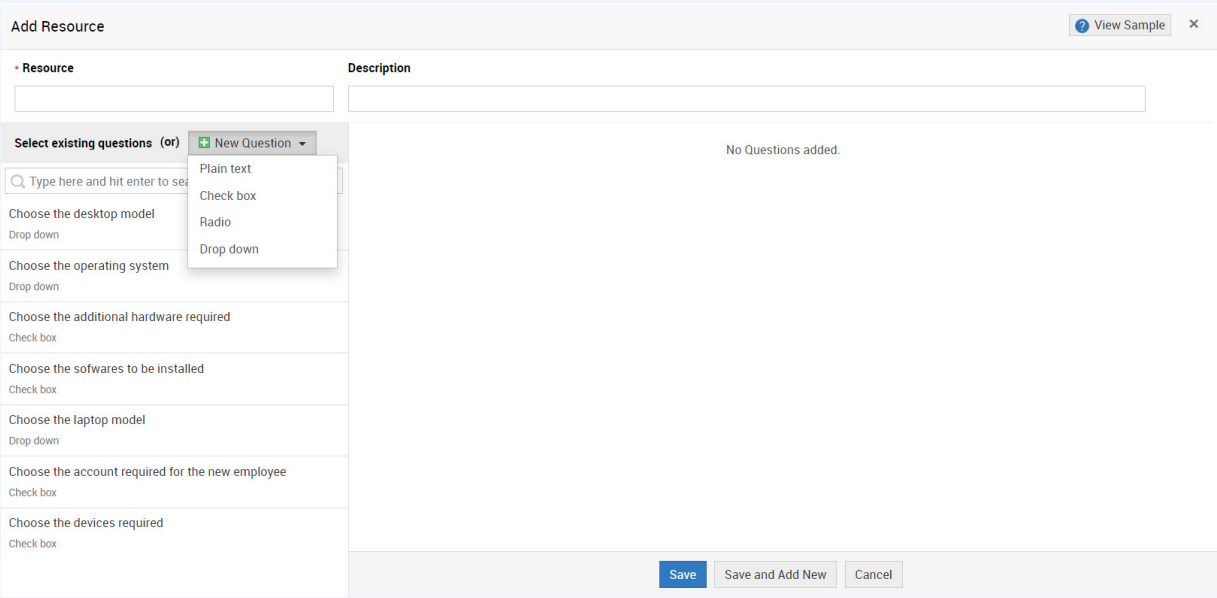

*Service request templates*



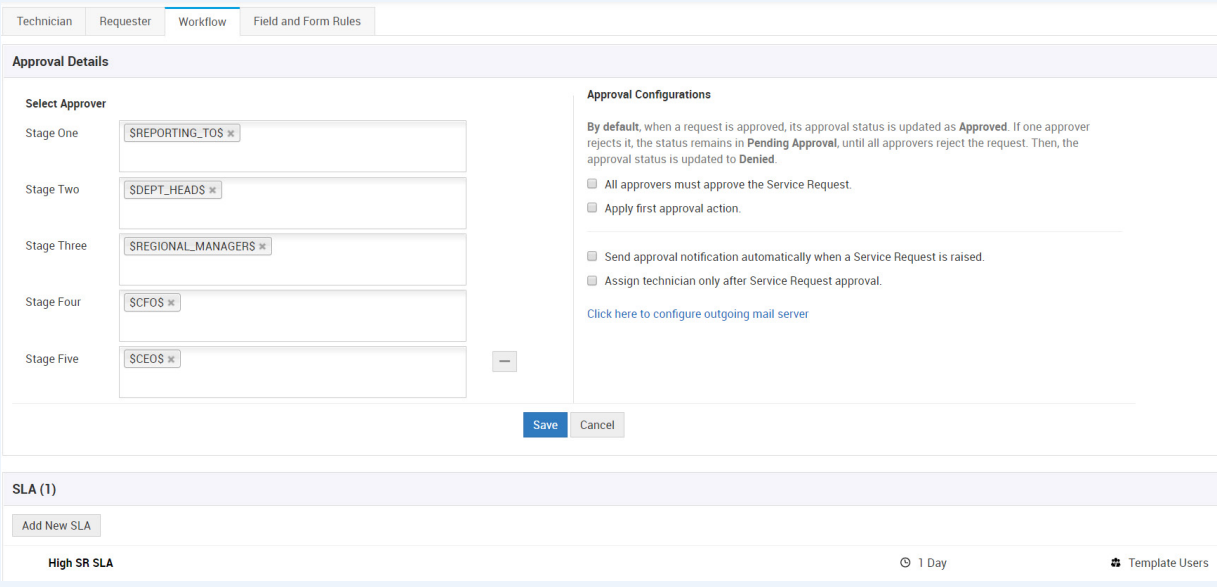

*Choose a laptop to find details*



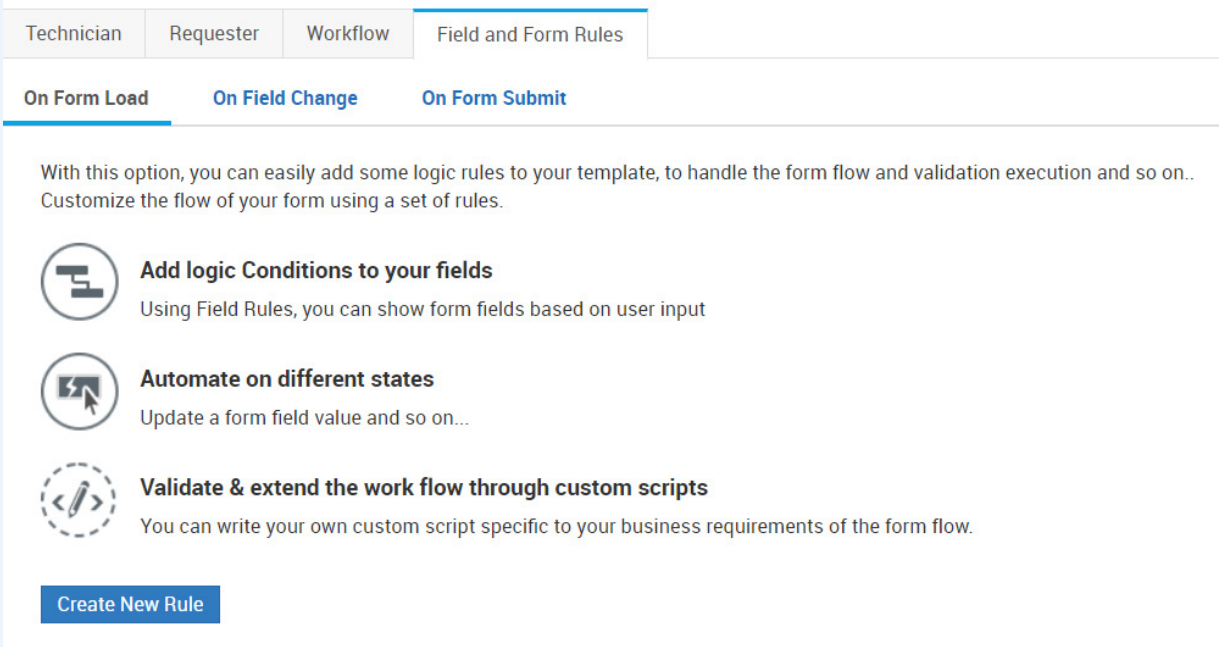

*Capture provisioning costs*




*Resource form for customization*




*Approval workflow and SLA*




*Field and form rules*

## 8.6.3 Problem management

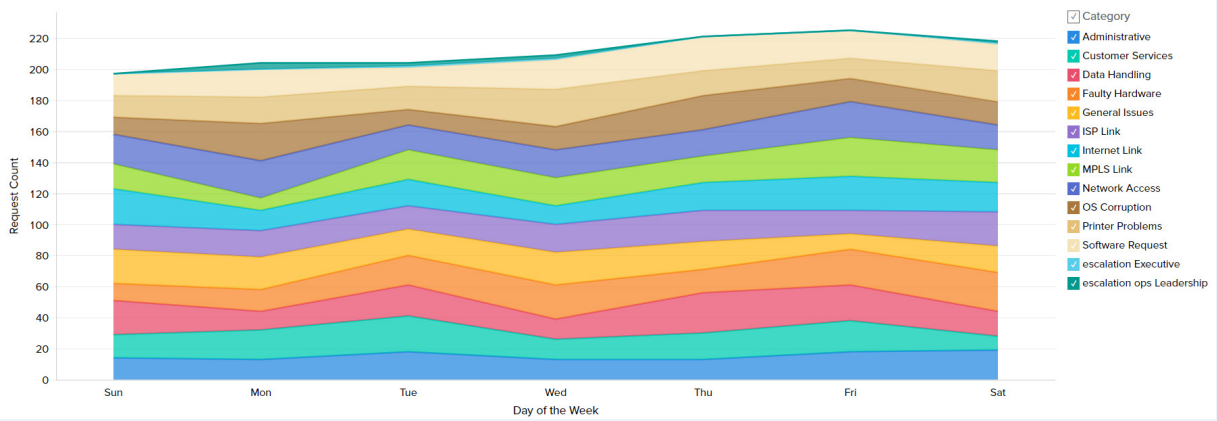
### Addressed process requirement(s):

- 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:

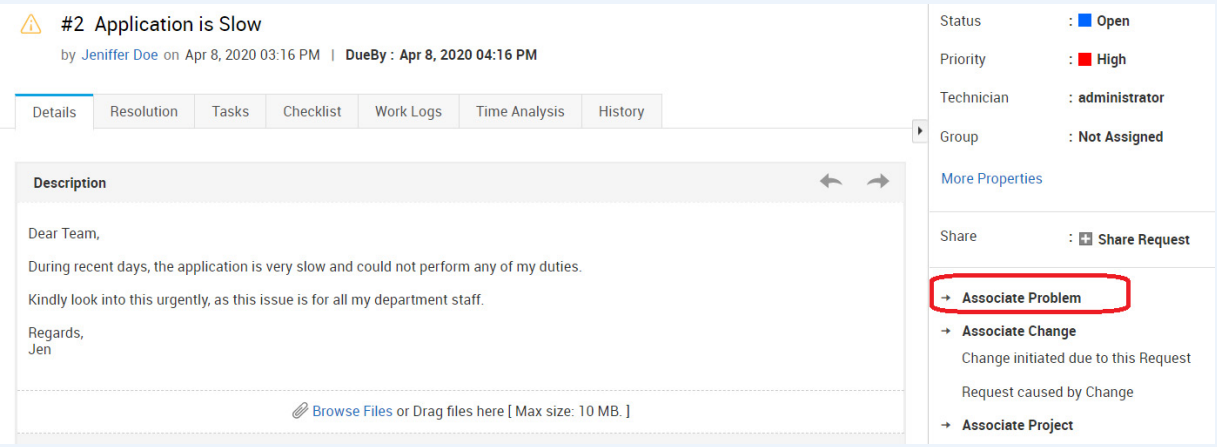
### ServiceDesk Plus and Analytics Plus

- The Reporting/Advanced Analytics module helps you to analyze data and trends on incidents to identify problems.



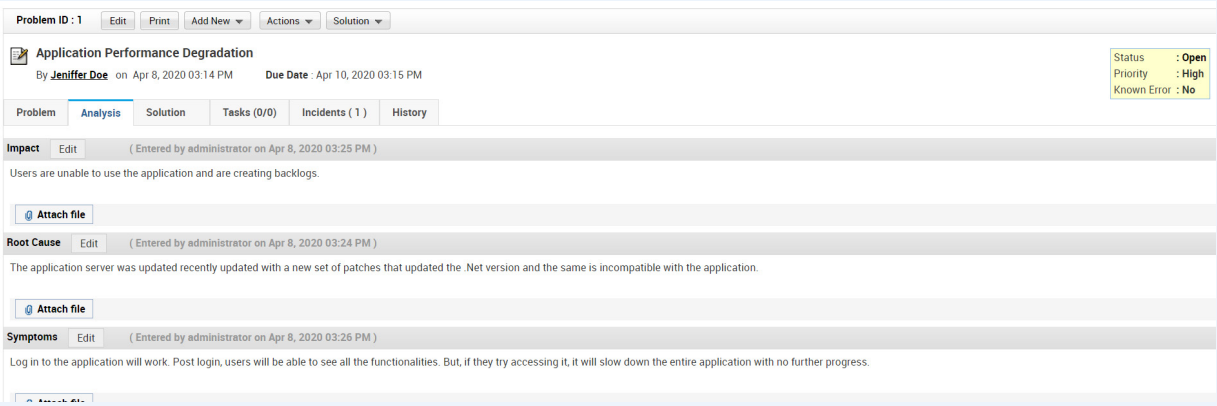

*Weekly ticket inflow by category*

- A problem record can be recorded, classified, prioritized, updated with actions, and resolved/closed. A problem record can be created directly after analyzing the incident trend or from a single incident or multiple reported open incidents.



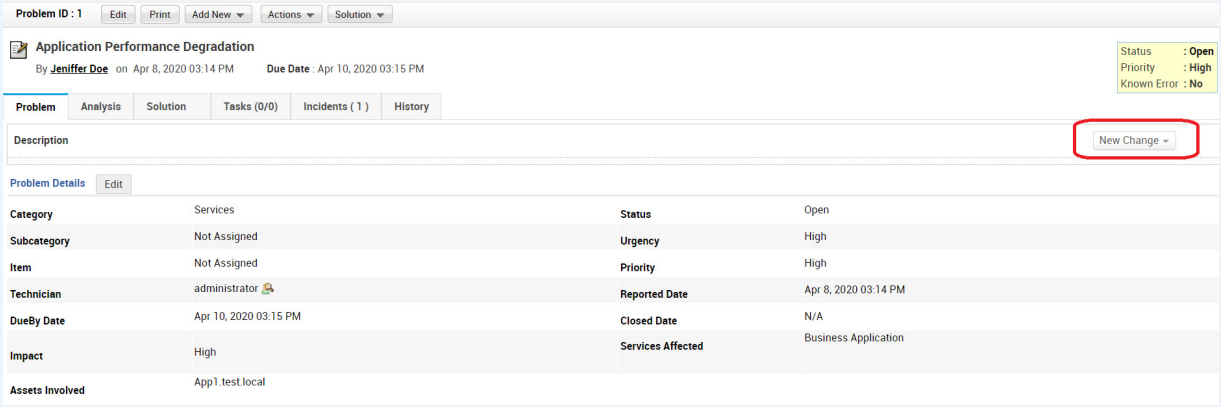

*Incident to problem association*

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



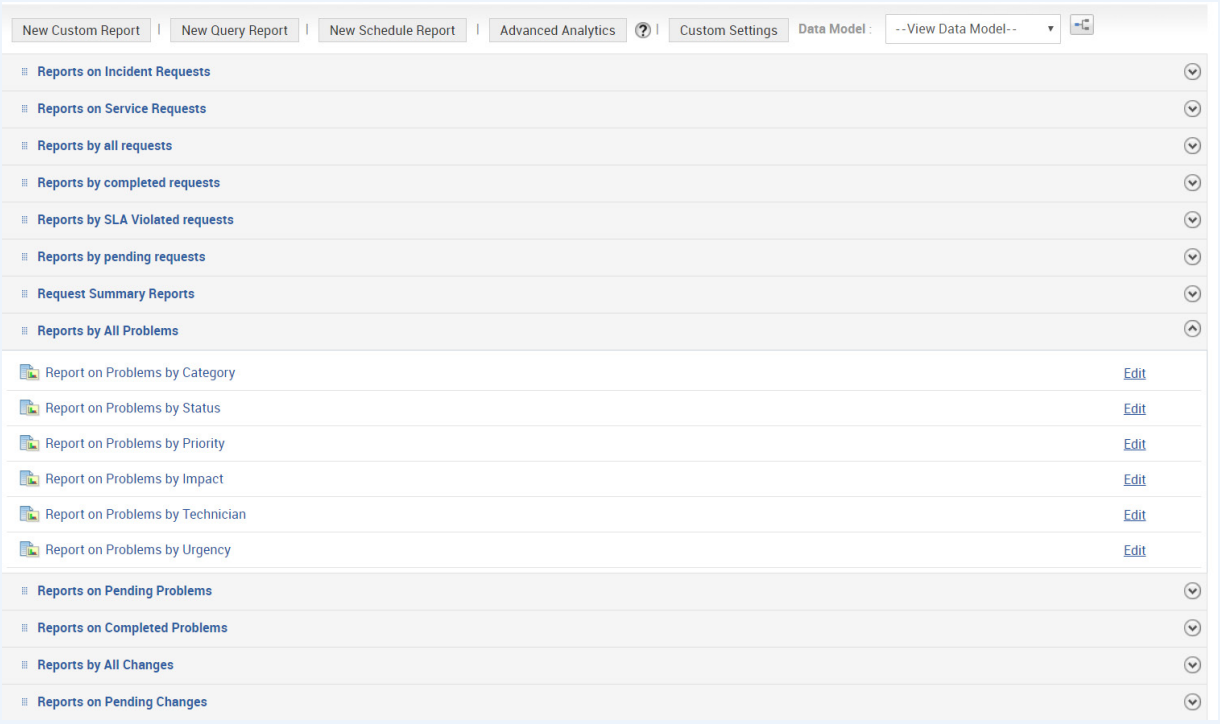

*Problem analysis*

- 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

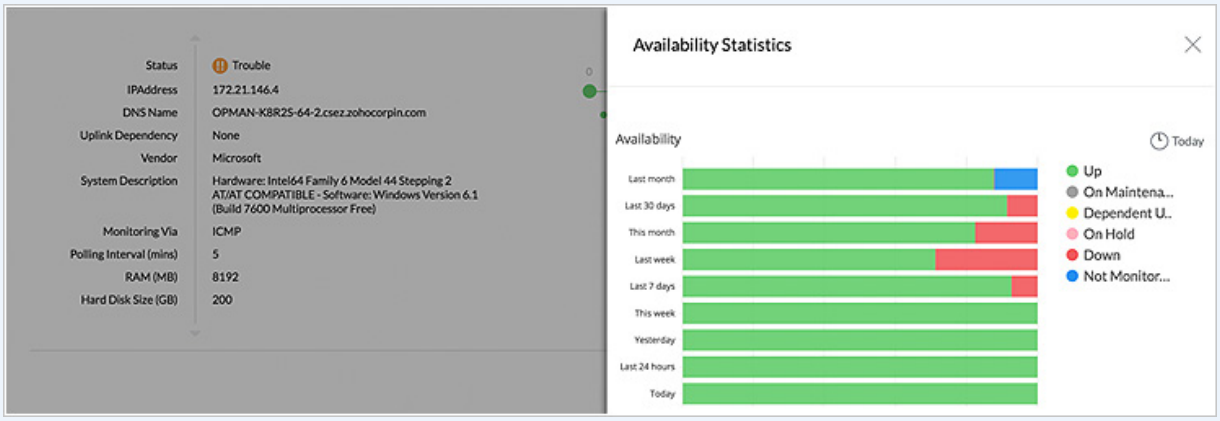
### Addressed process requirement(s):

- 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.

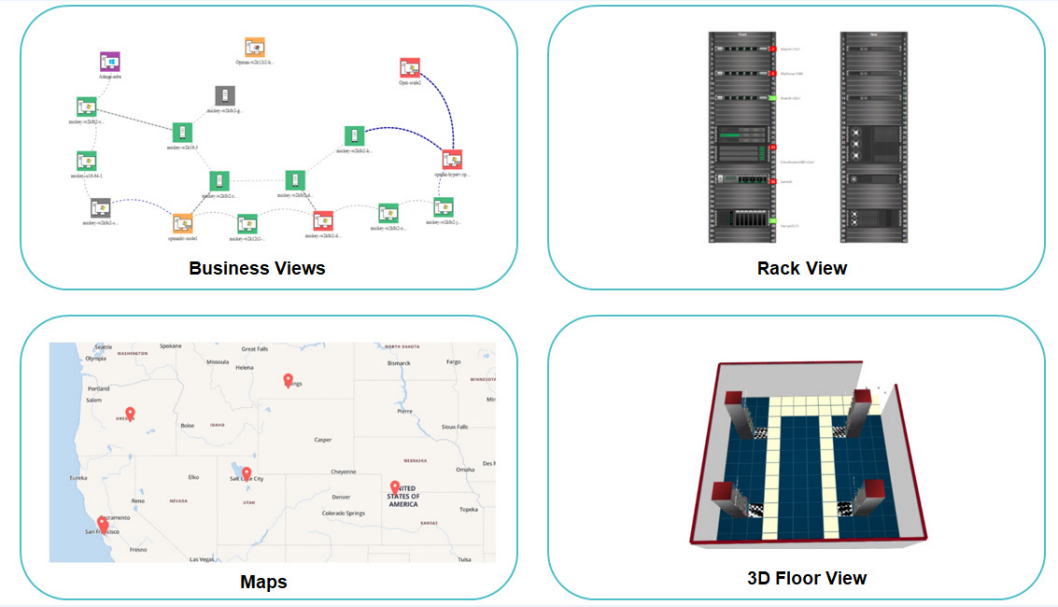
### ManageEngine product that can help in implementing these processes:

**OpManager Plus and Applications Manager**

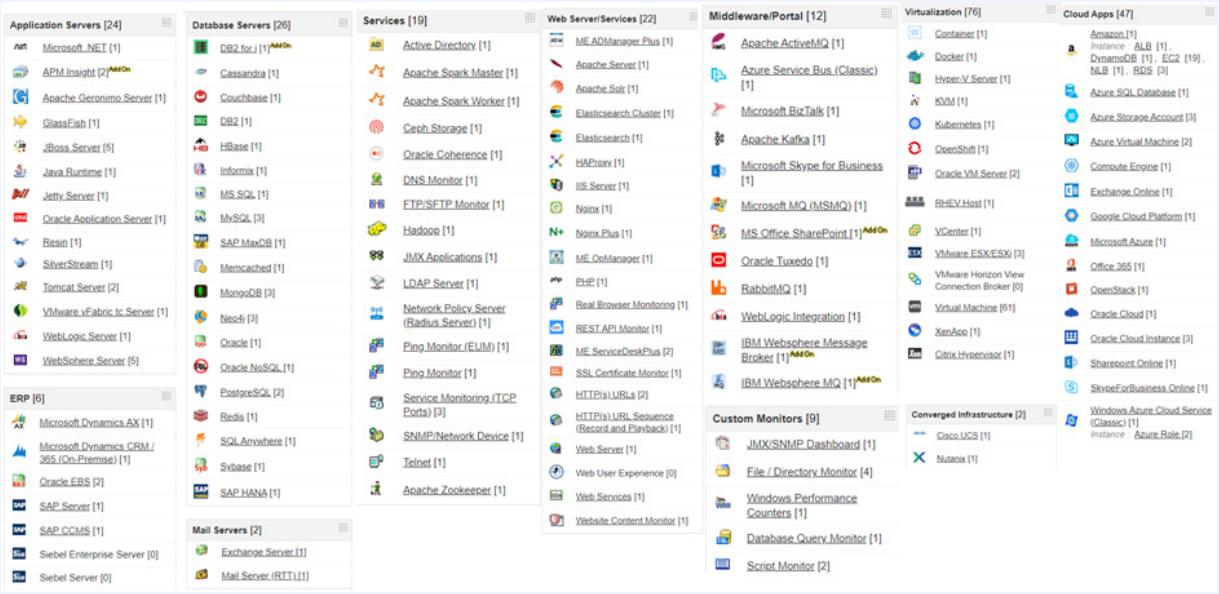
- Monitor the service availability based on all the dependent service components including network, servers, virtualization, storage, applications, databases, and websites, and compare them against the agreed target.



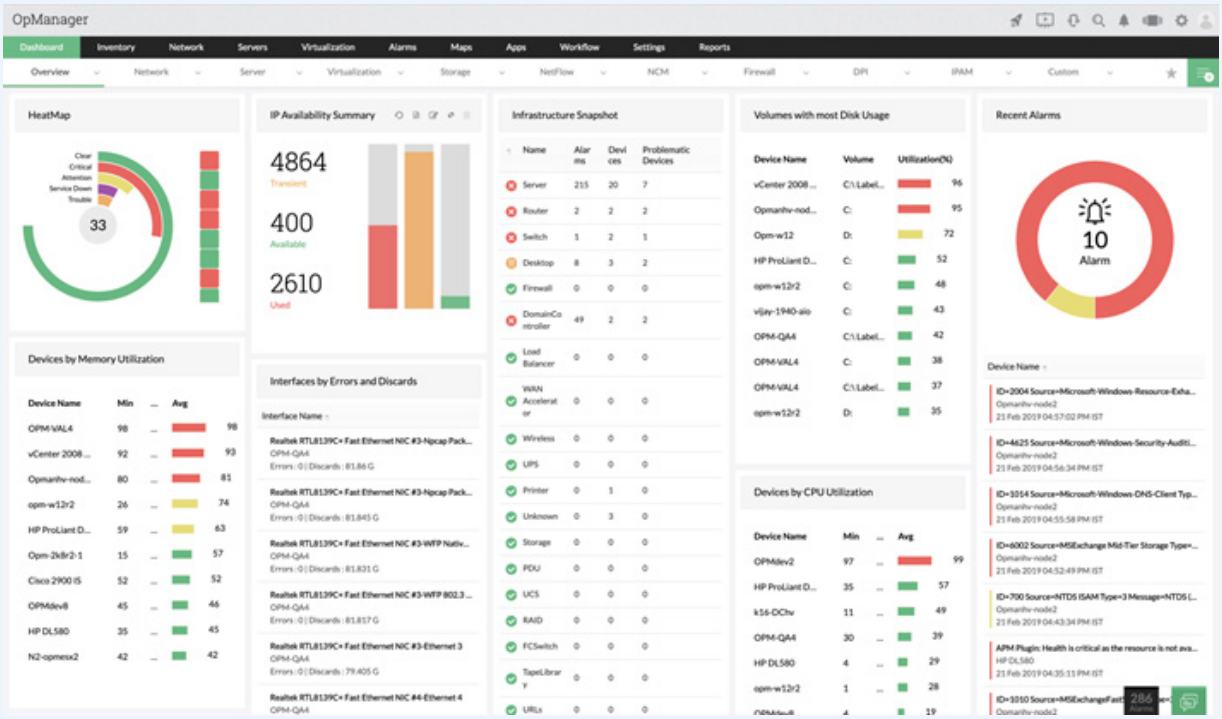

*Availability statistics*




*Availability representation*

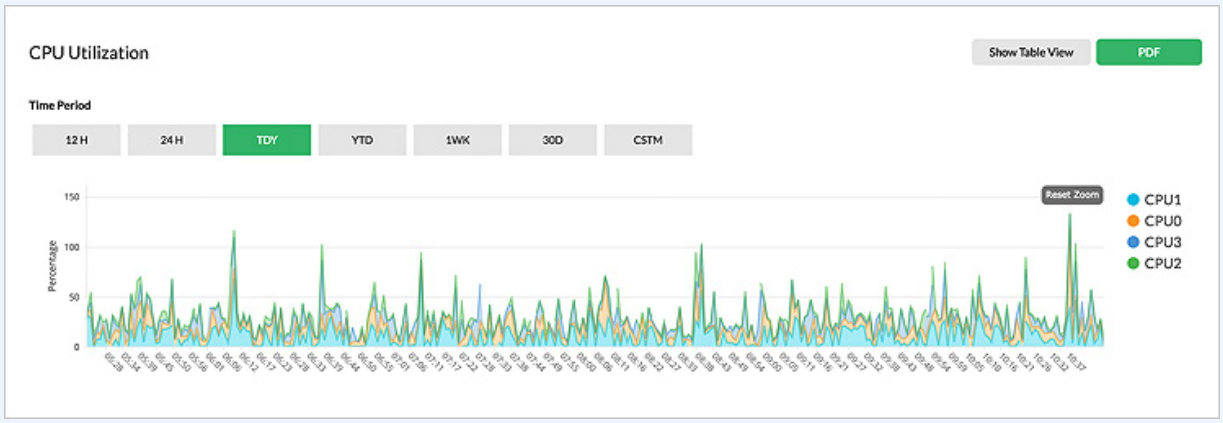



*Applications monitoring*

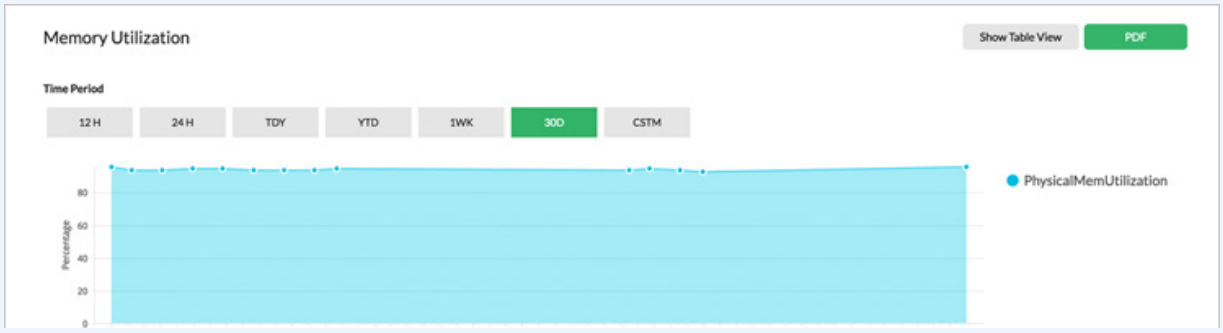



*Monitoring dashboard*

- 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.

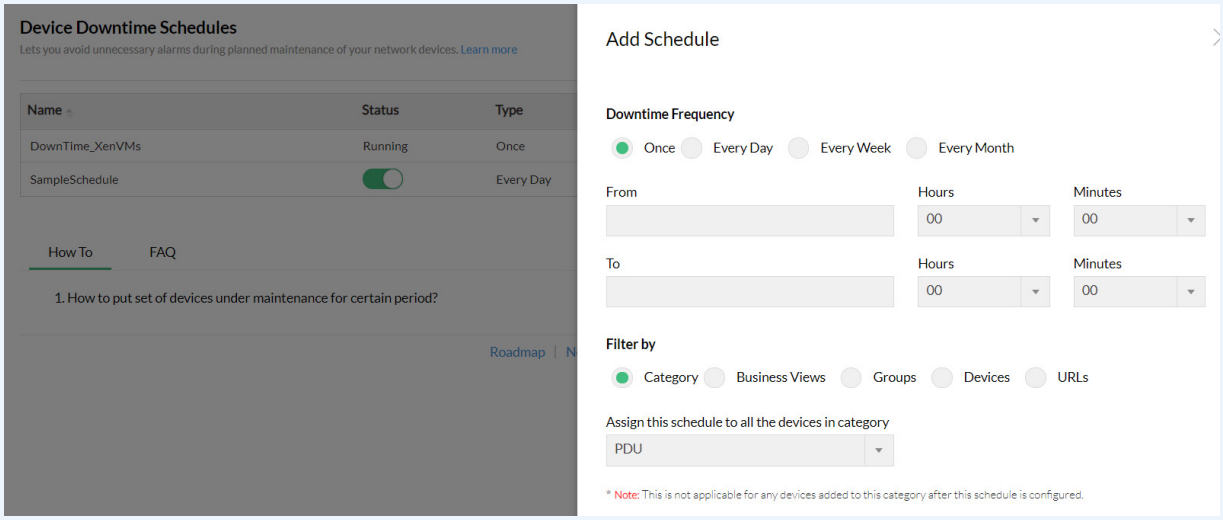



*Performance monitoring: CPU*

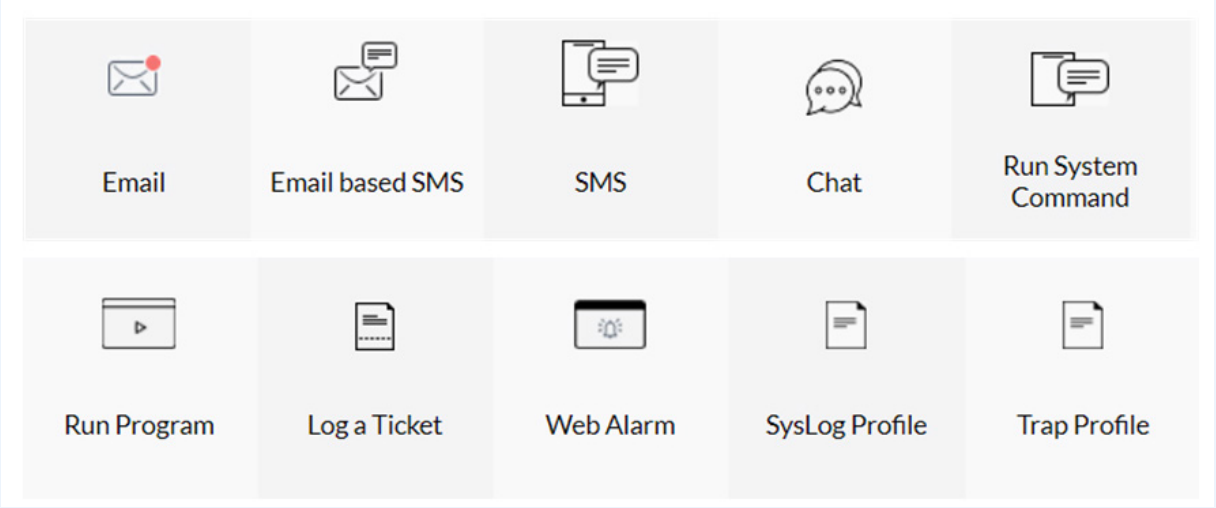



*Performance monitoring: Memory*

- 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

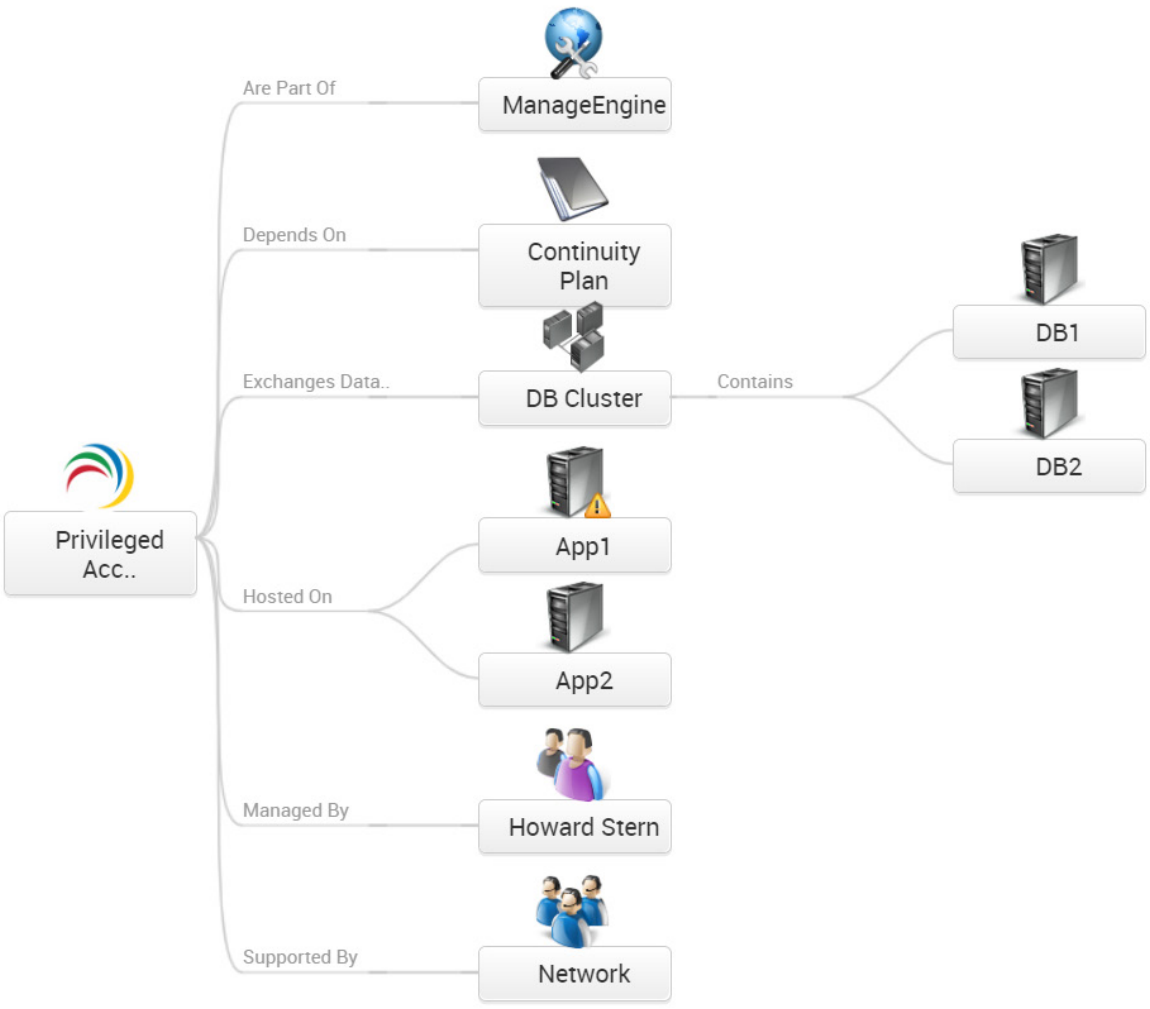
**Addressed process requirement(s):**

- 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 processes:**

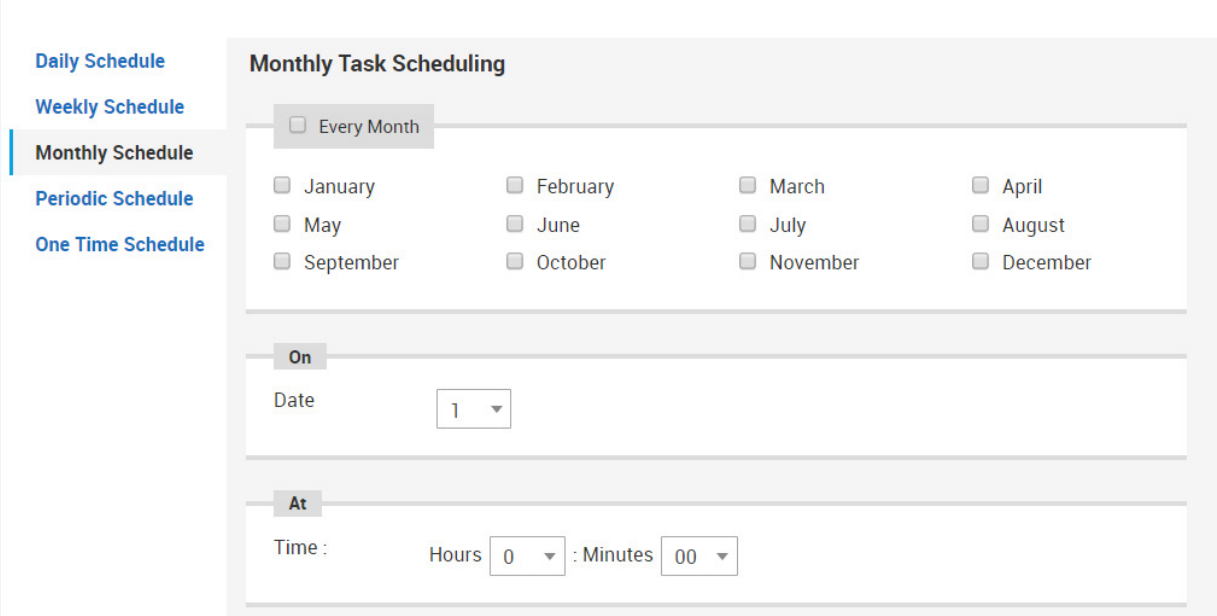
## ServiceDesk Plus

- 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.

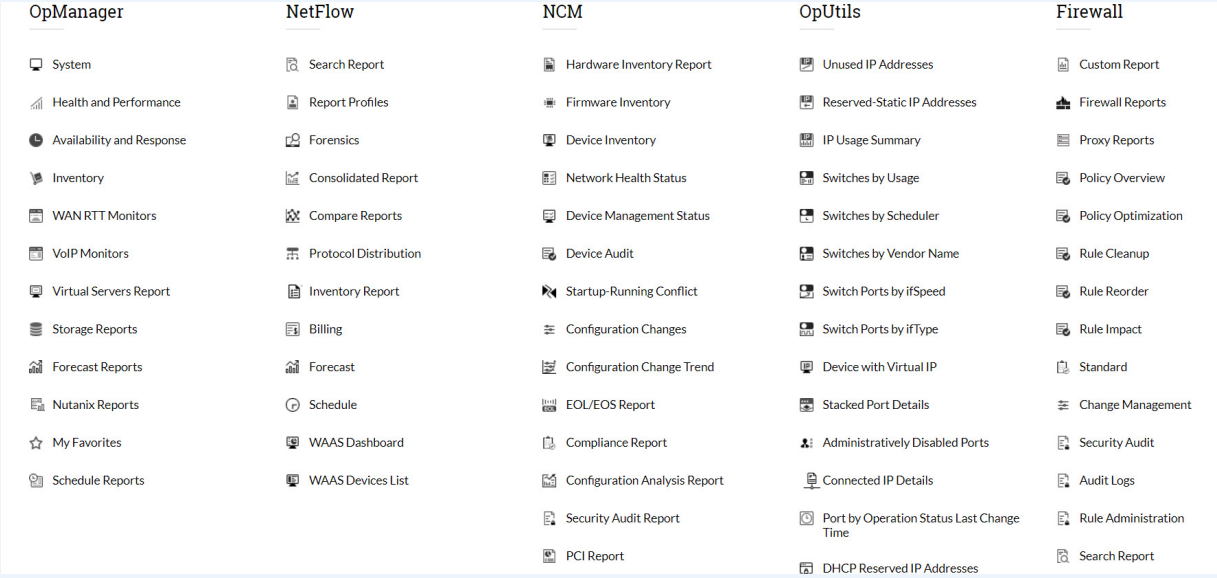



*Preventive maintenance schedule*

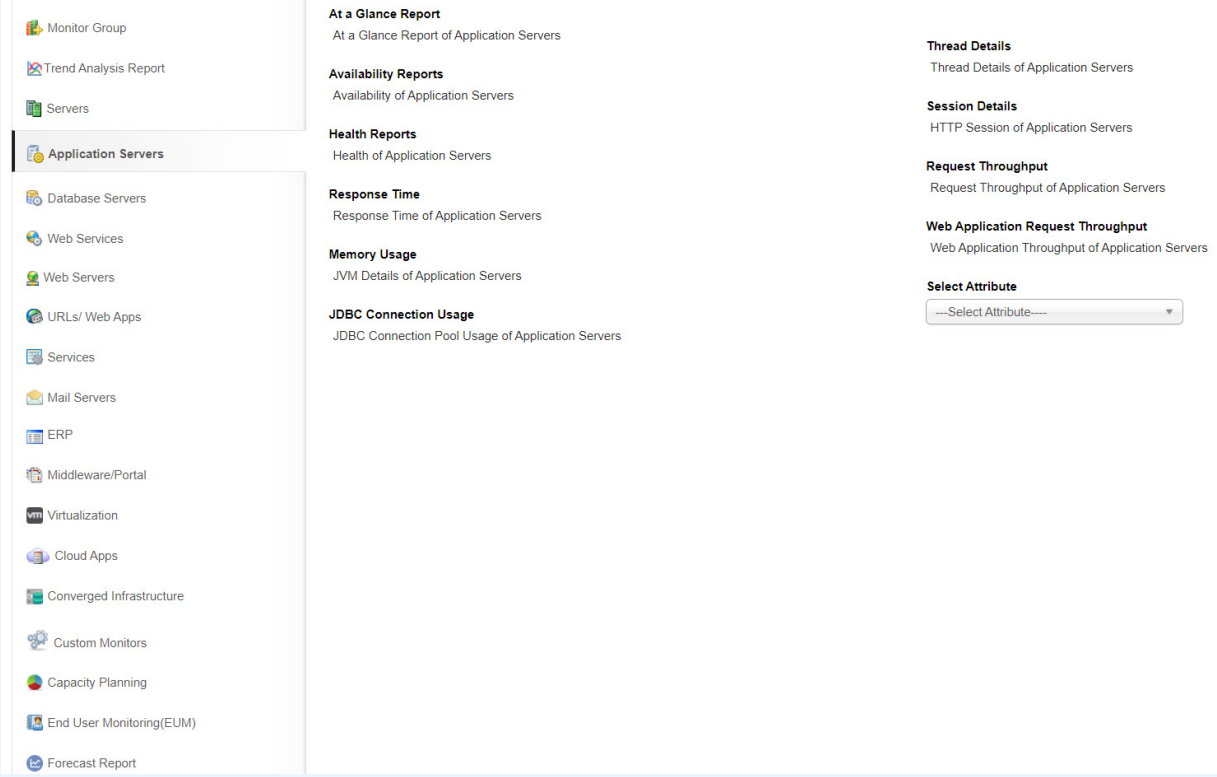
- As part of the change/release management process in ServiceDesk Plus, testing the continuity plan can be made a mandatory task for all major changes. The cause, impact, and recovery when the continuity plan has been invoked can be documented as part of the same.

## 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 reports*




*Reports in Applications Manager*

## 8.7.3 Information security management

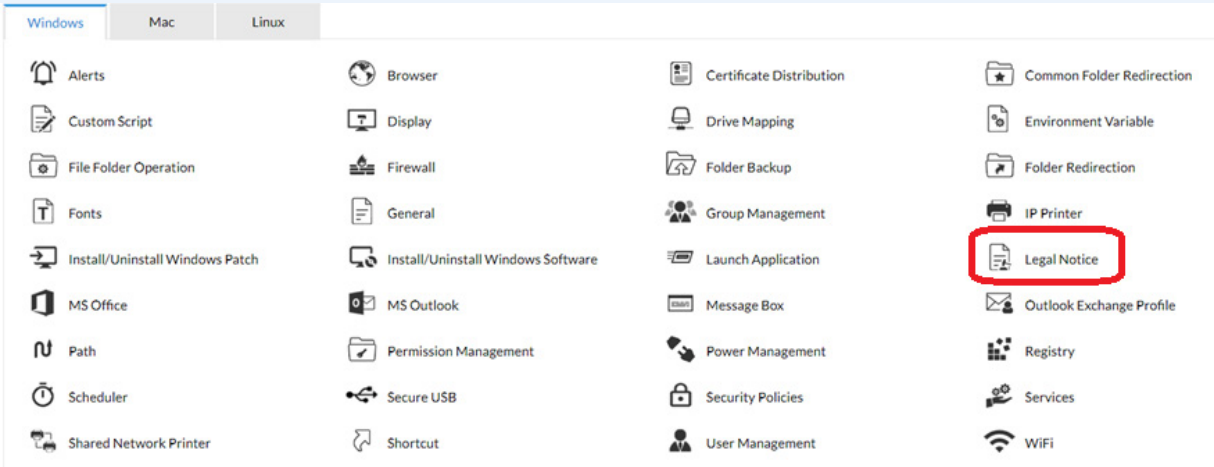
### Addressed process requirement(s):

- 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 improvement.

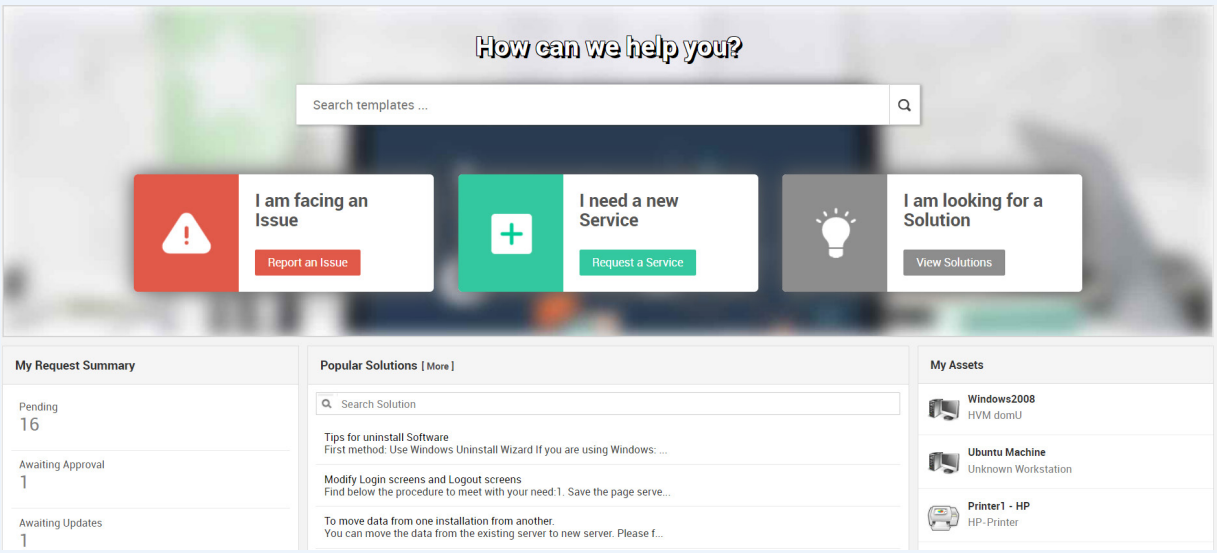
### ManageEngine products that can help in implementing these processes:

### 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.

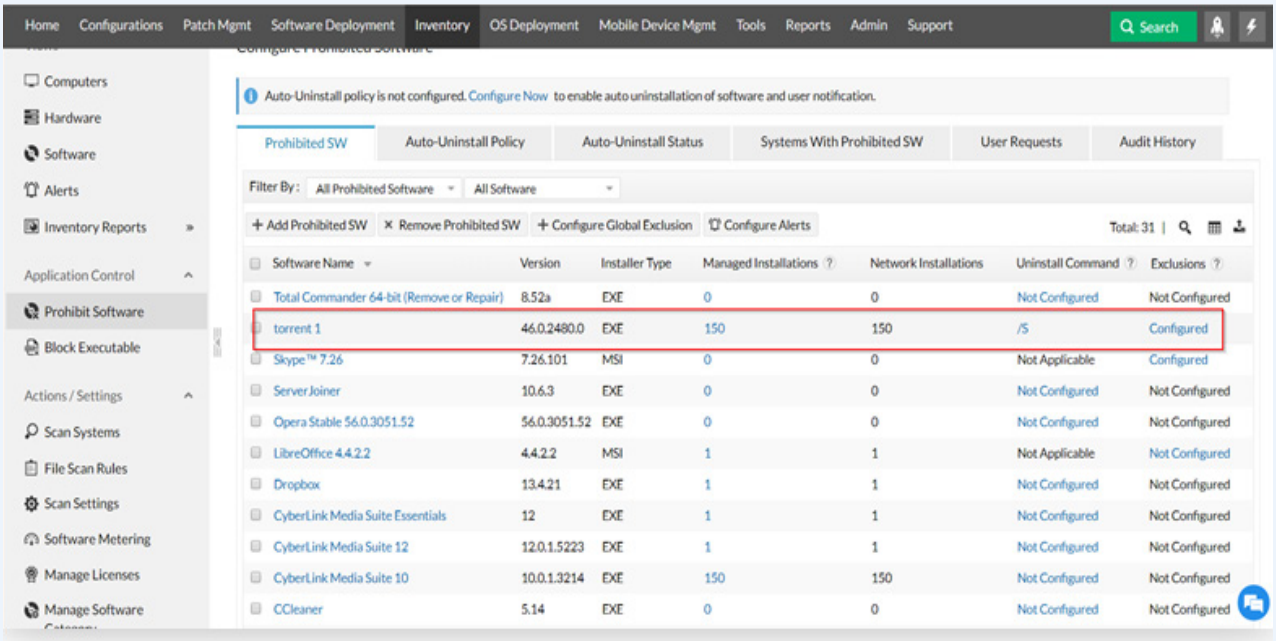



*Endpoint Central: Manage configurations*

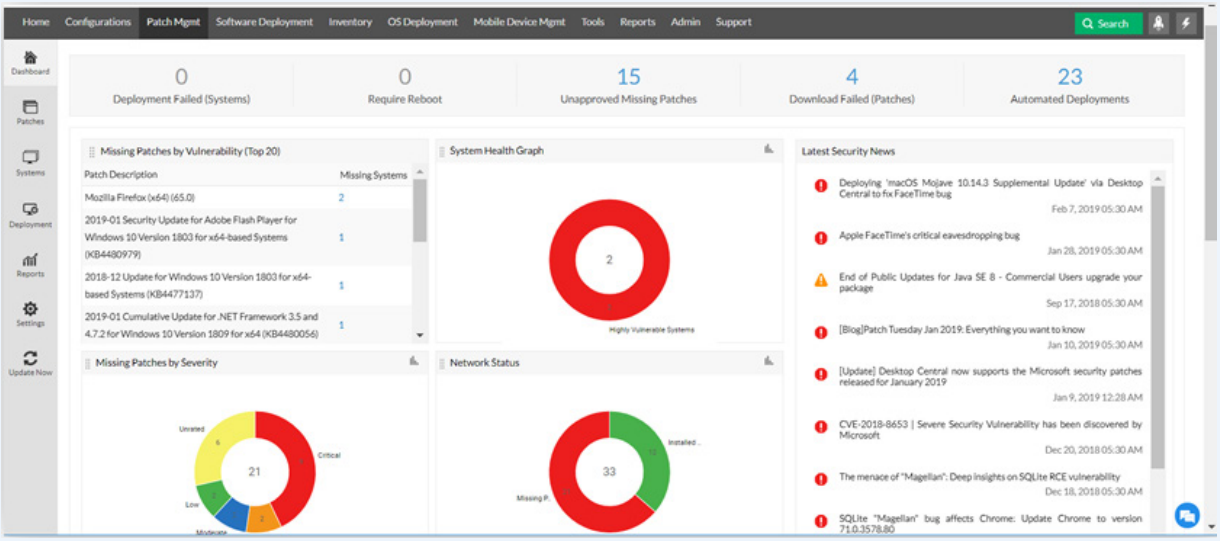



*ServiceDesk Plus: Self-service portal*

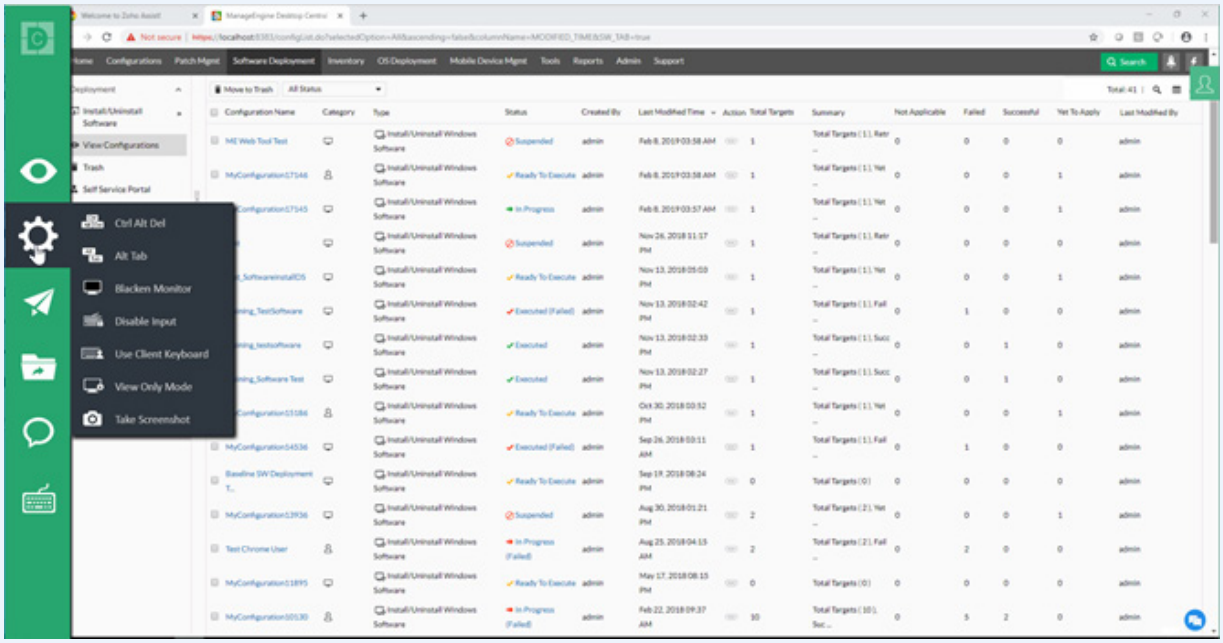
- Deploy the security controls required on endpoints like prohibiting specific software installation, blocking executables, blocking USBs, patching, recording the remote sessions, and securing mobile devices, browsers, and so on.



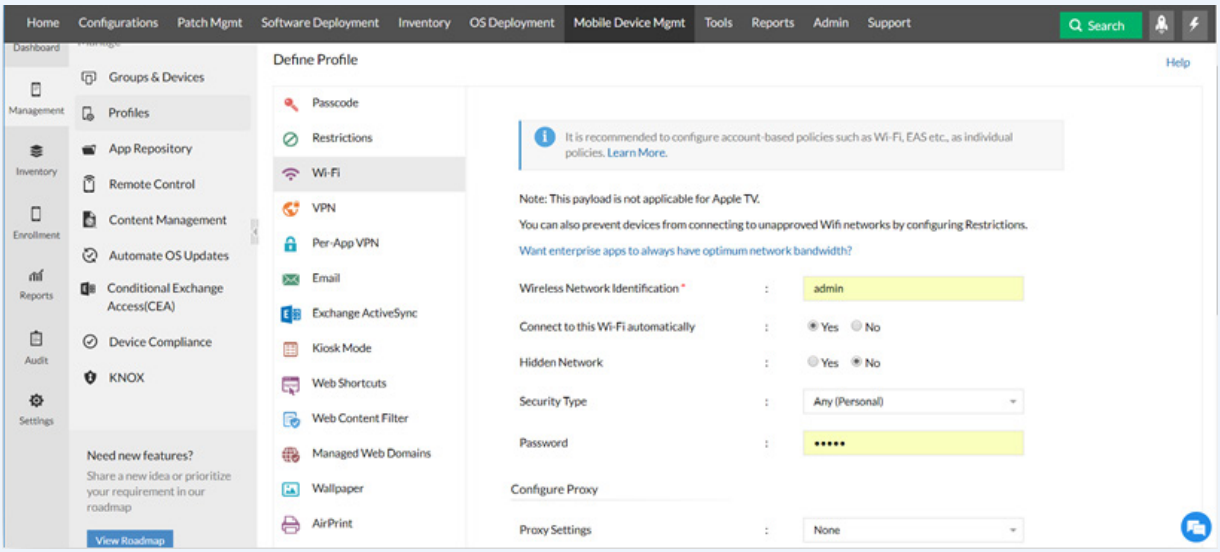

*Endpoint Central: Control software and executable installation*



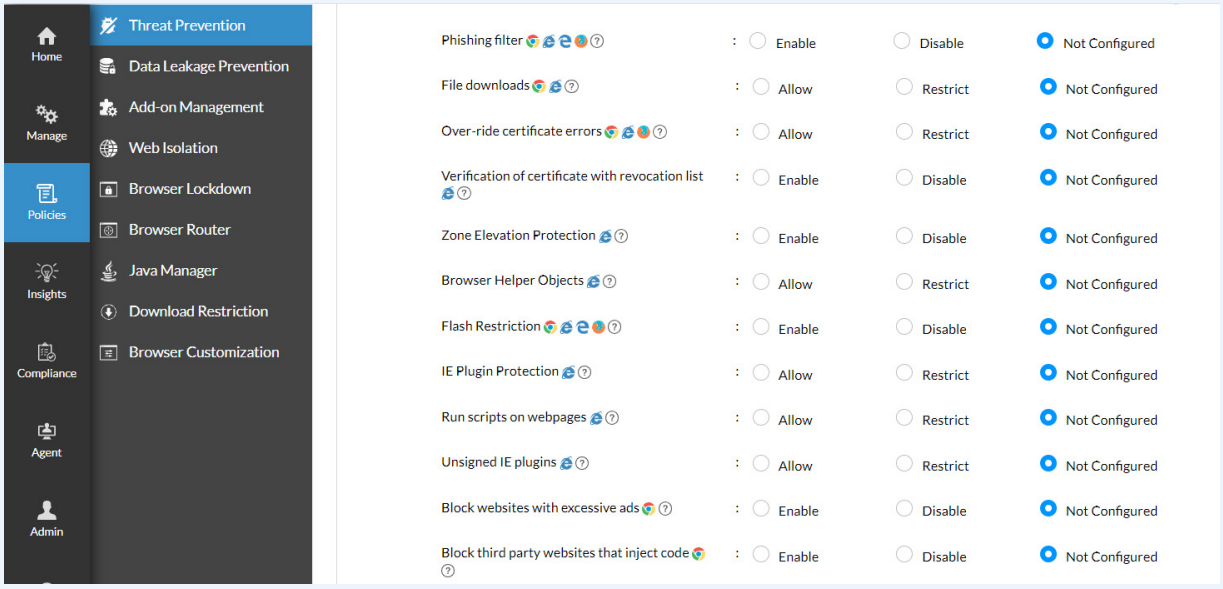

*Endpoint Central: Comprehensive patch management*




*Endpoint Central: Recorded remote sessions*



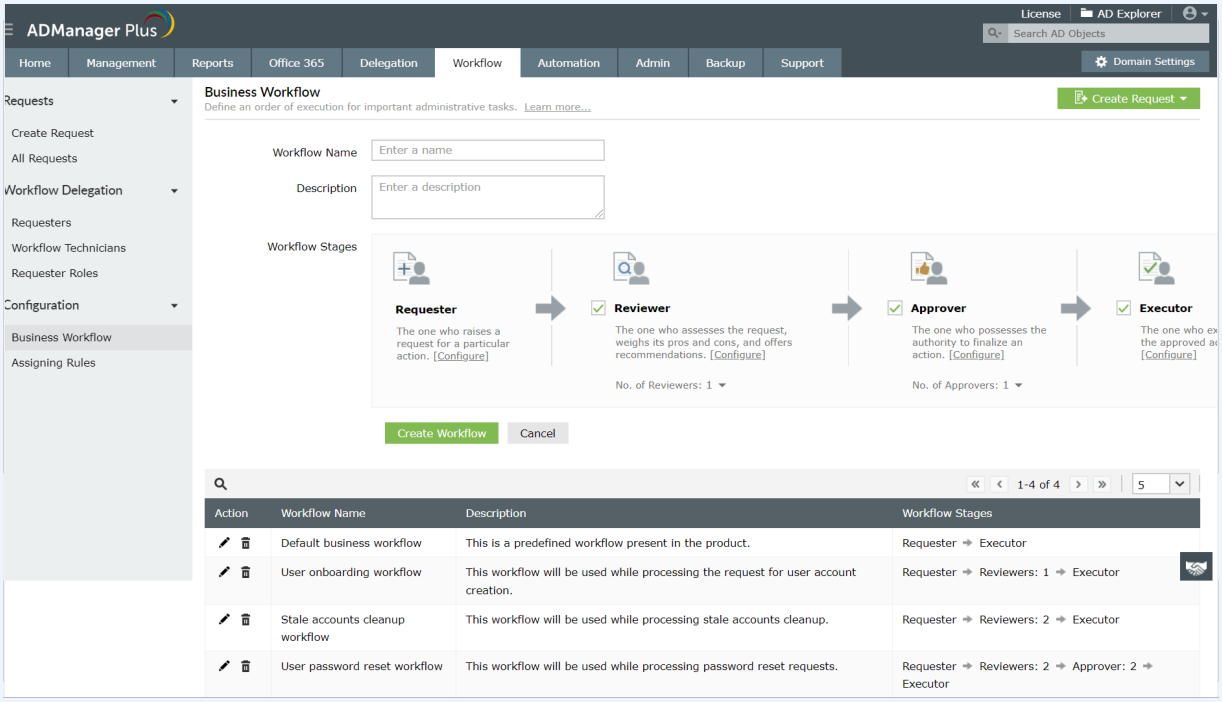

*Endpoint Central: Securing mobile devices*



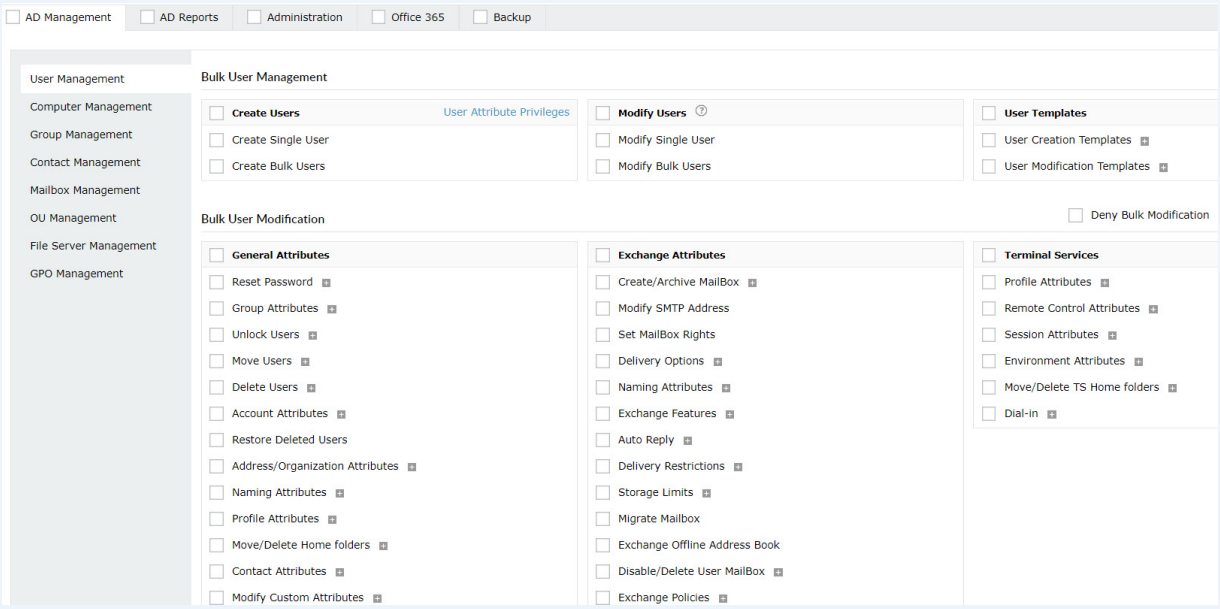

*Browser risk management*

## AD360

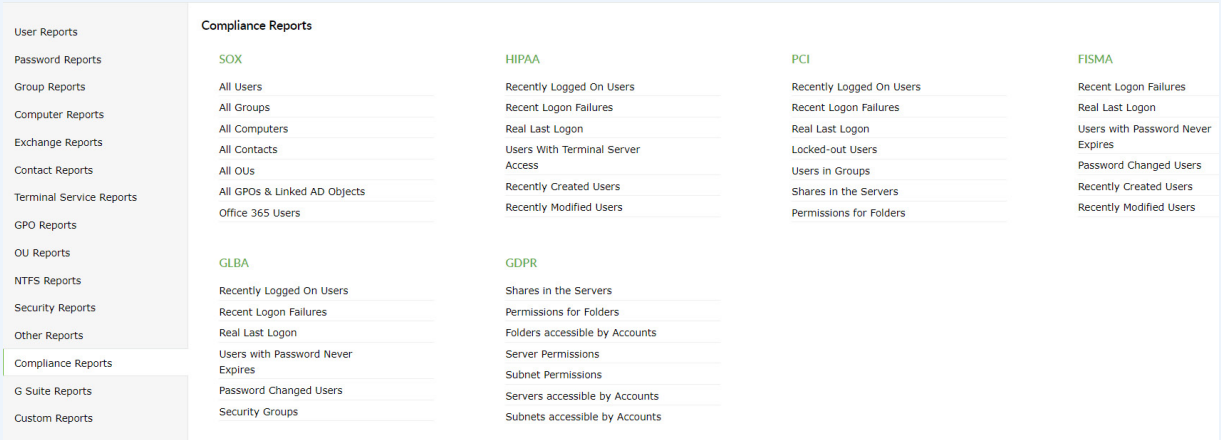
- Deploy the security controls required for accessing and managing Active Directory, Exchange, and Microsoft 365 securely through the delegated capabilities. It also helps to deploy required controls for users to change/reset the password, unlock accounts through multiple identity verification methods,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



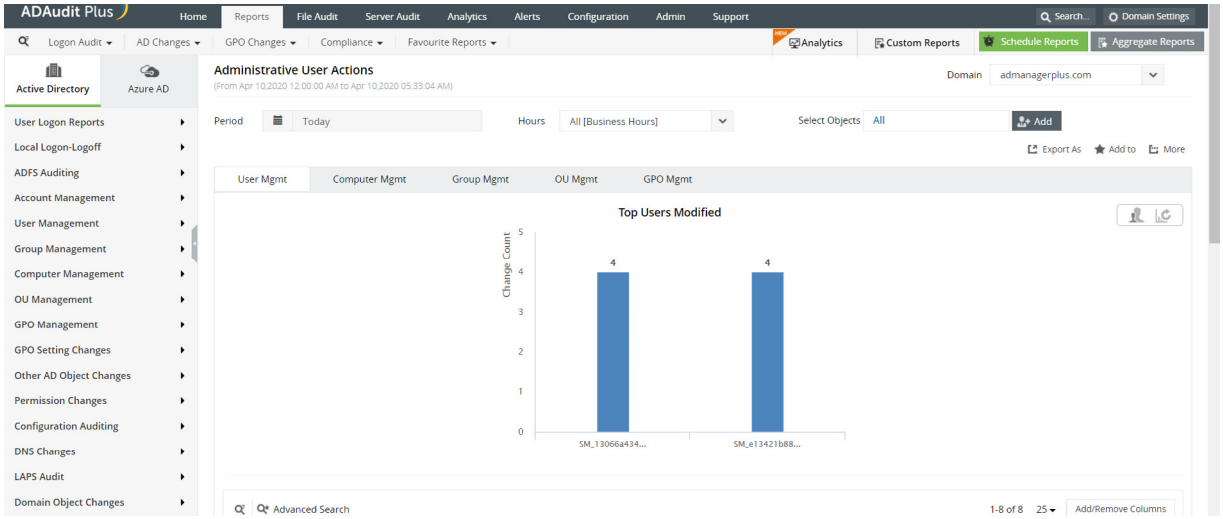

*Commit changes in AD on approval*



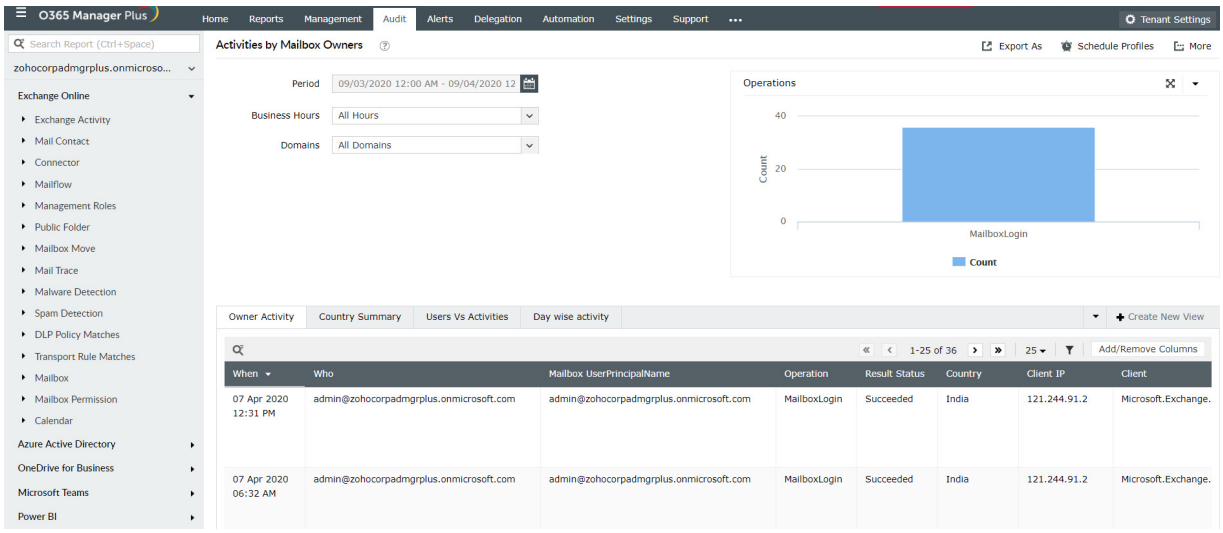

*Delegate access for AD management*



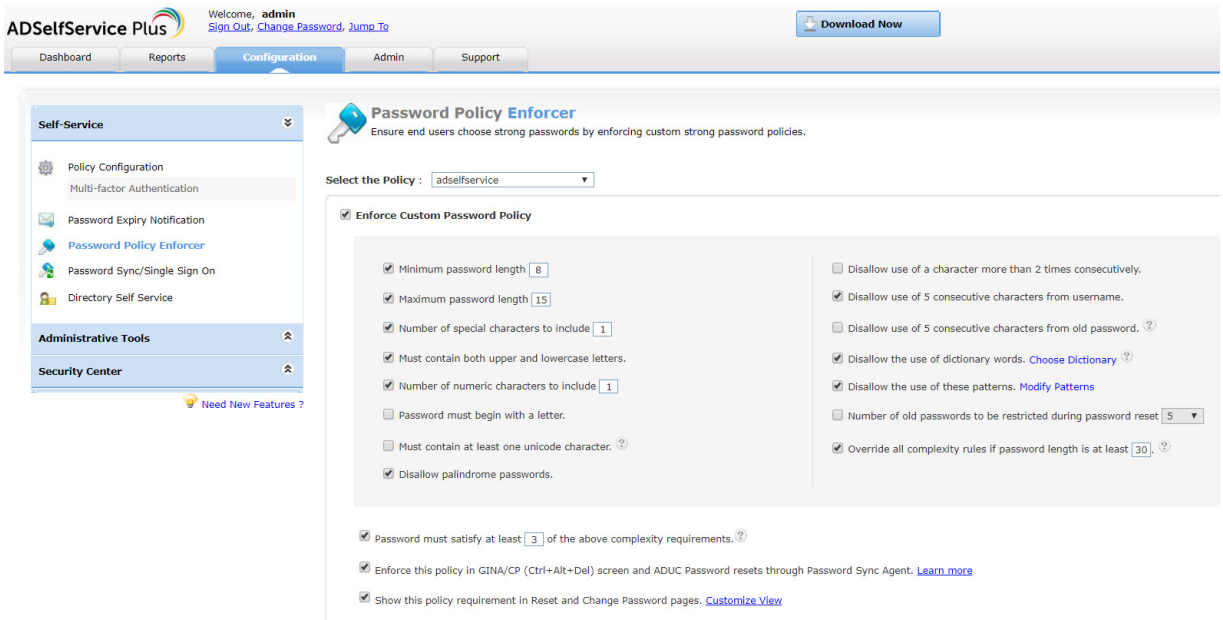

*Compliance reports for AD management*



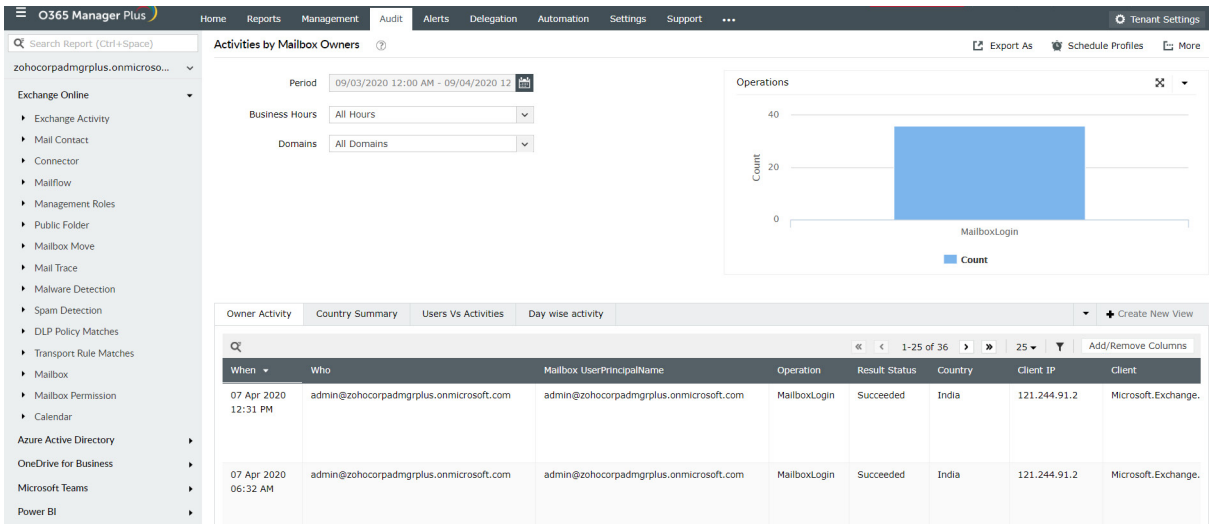

*AD and file server change auditing*



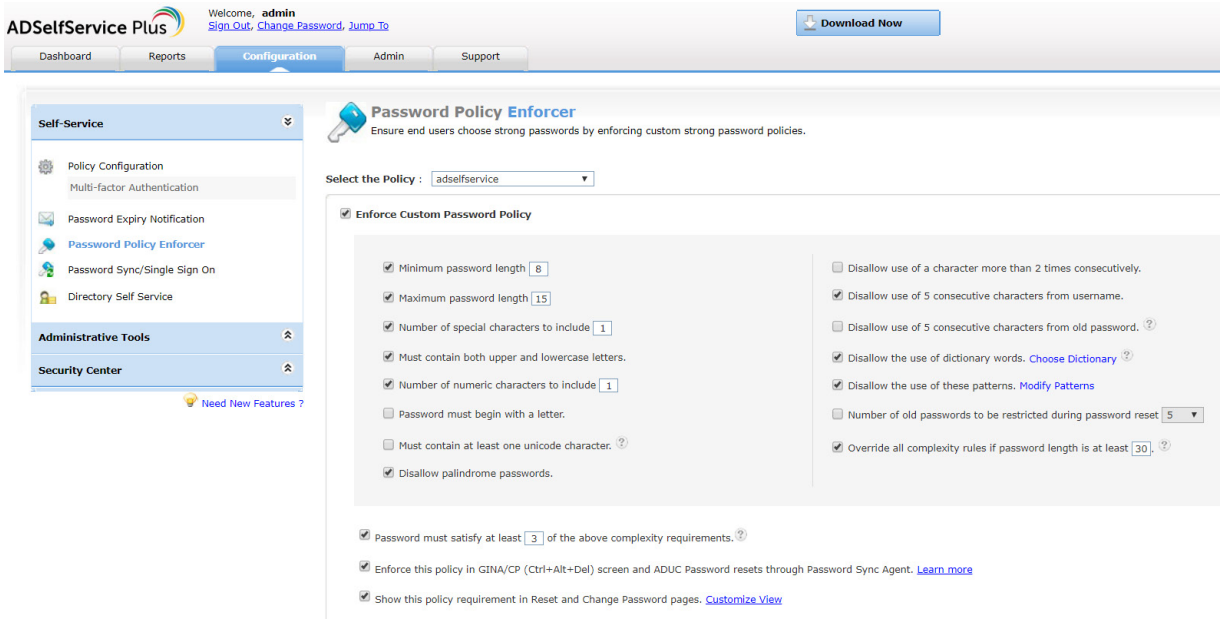

*M365 management auditing and reporting*



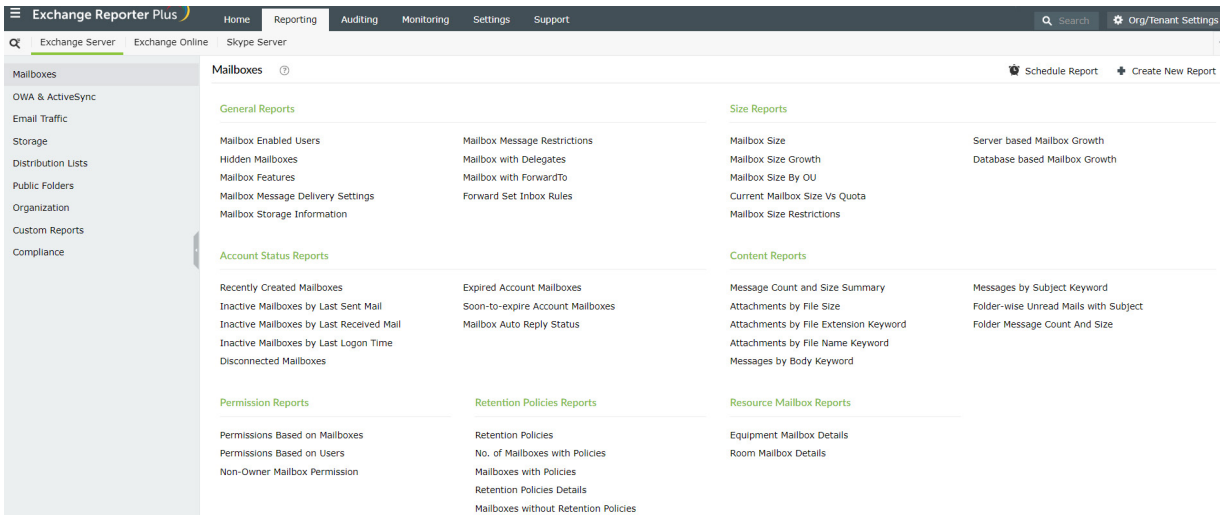

*Securely self manage passwords and accounts*




*M365 management auditing and reporting*




*Securely self manage passwords and accounts*

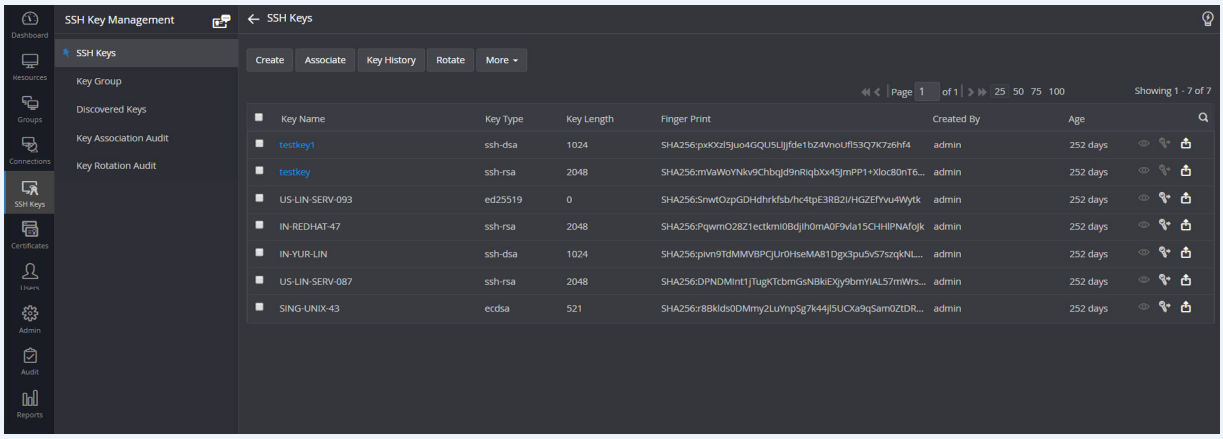



*Exchange auditing and reporting*

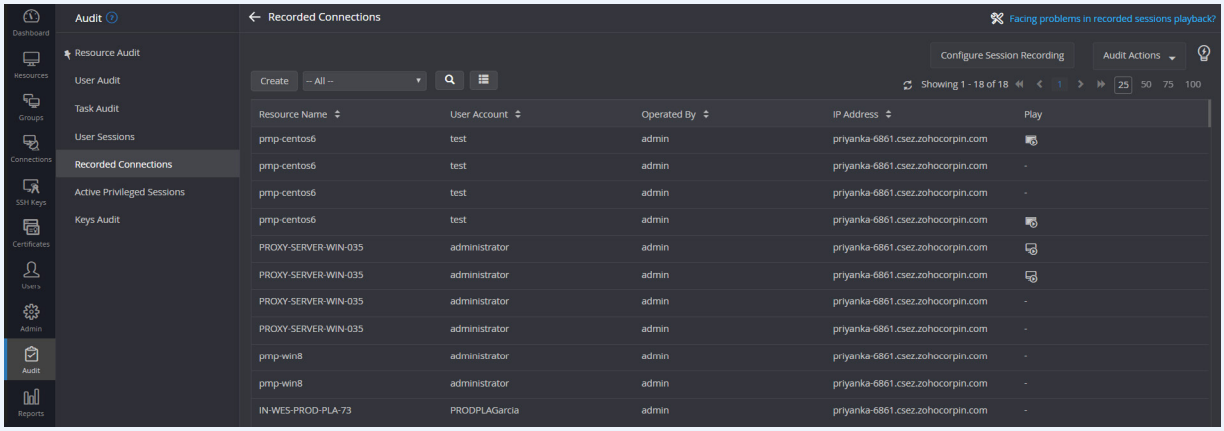
## PAM360

- 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.

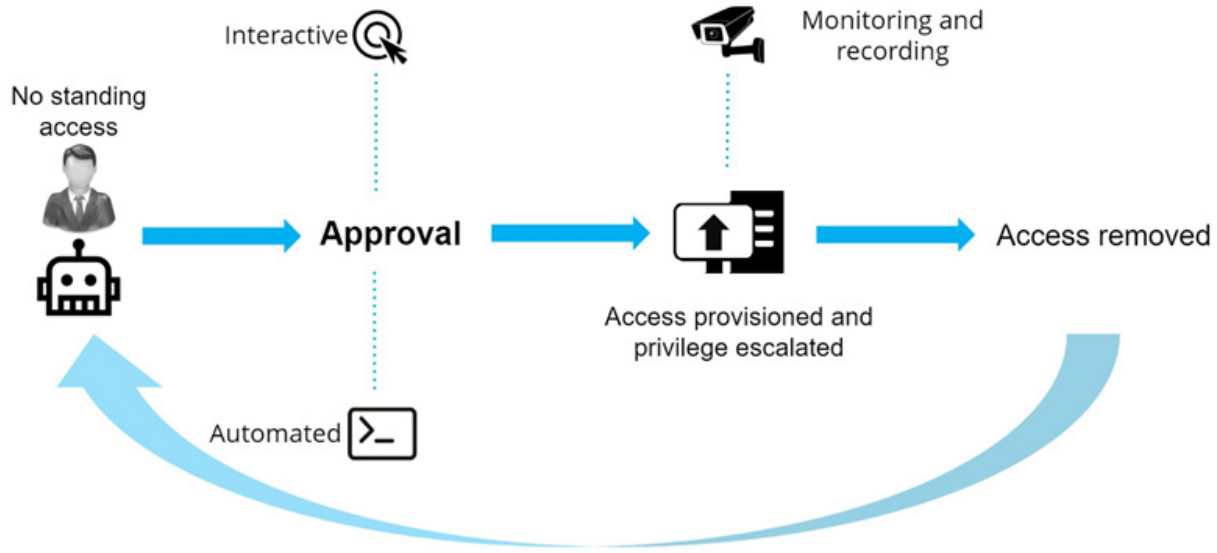

*Secured privileged password management*




*SSL/SSH key management*

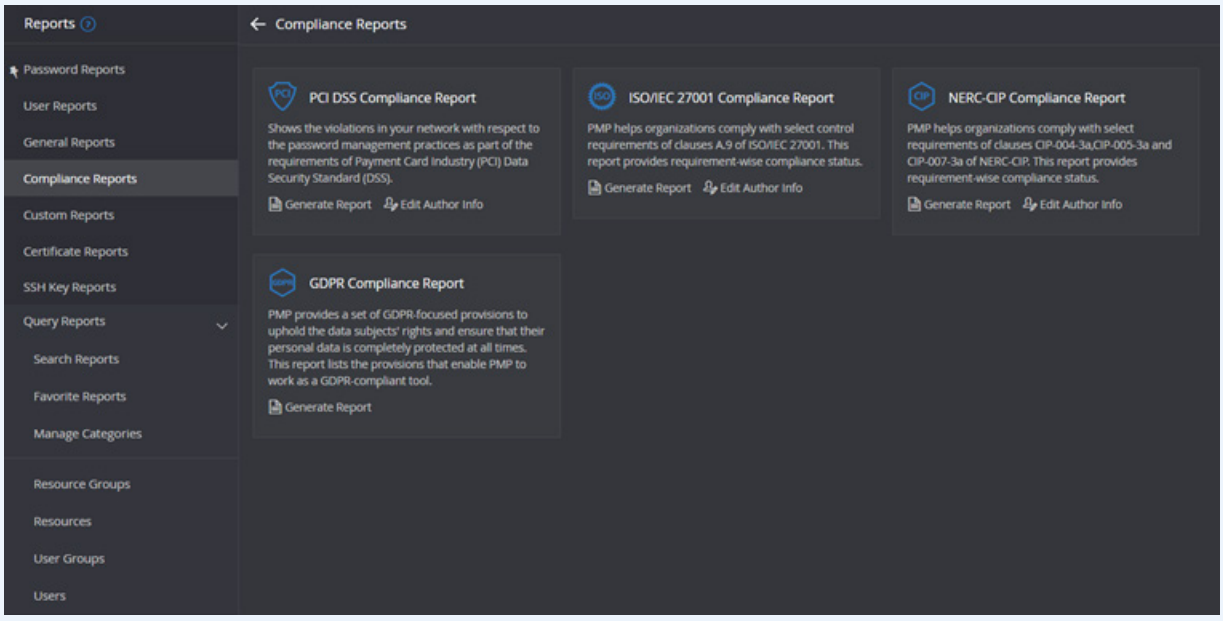



*Activity audit: Recorded sessions*




*Just-in-time privilege escalation*

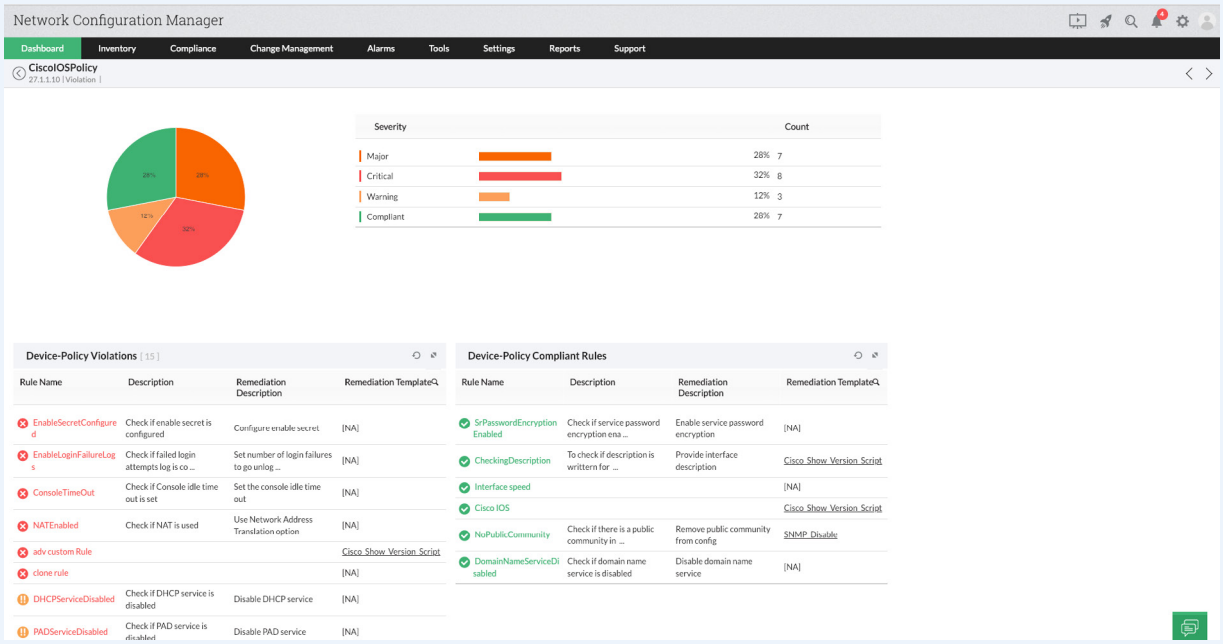
- The stored password can be changed post access or periodically using the configured password policy. It provides reporting on ISO 27001 as well by default.




*Compliance reports*

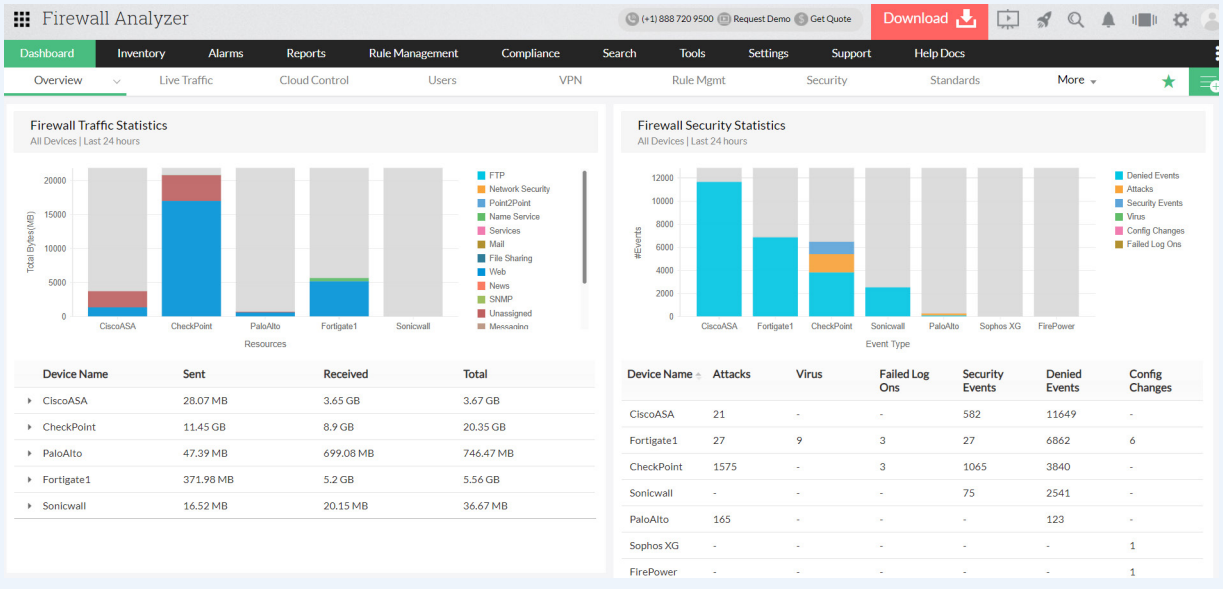
## OpManager Plus

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

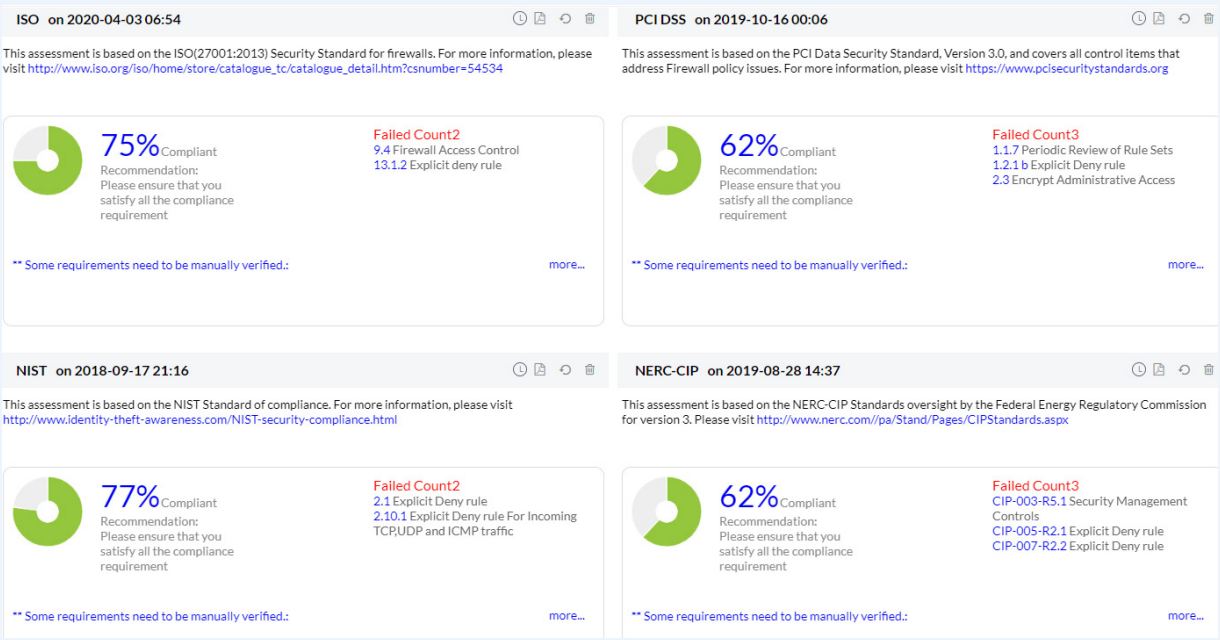



*Compliance check for network devices*

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



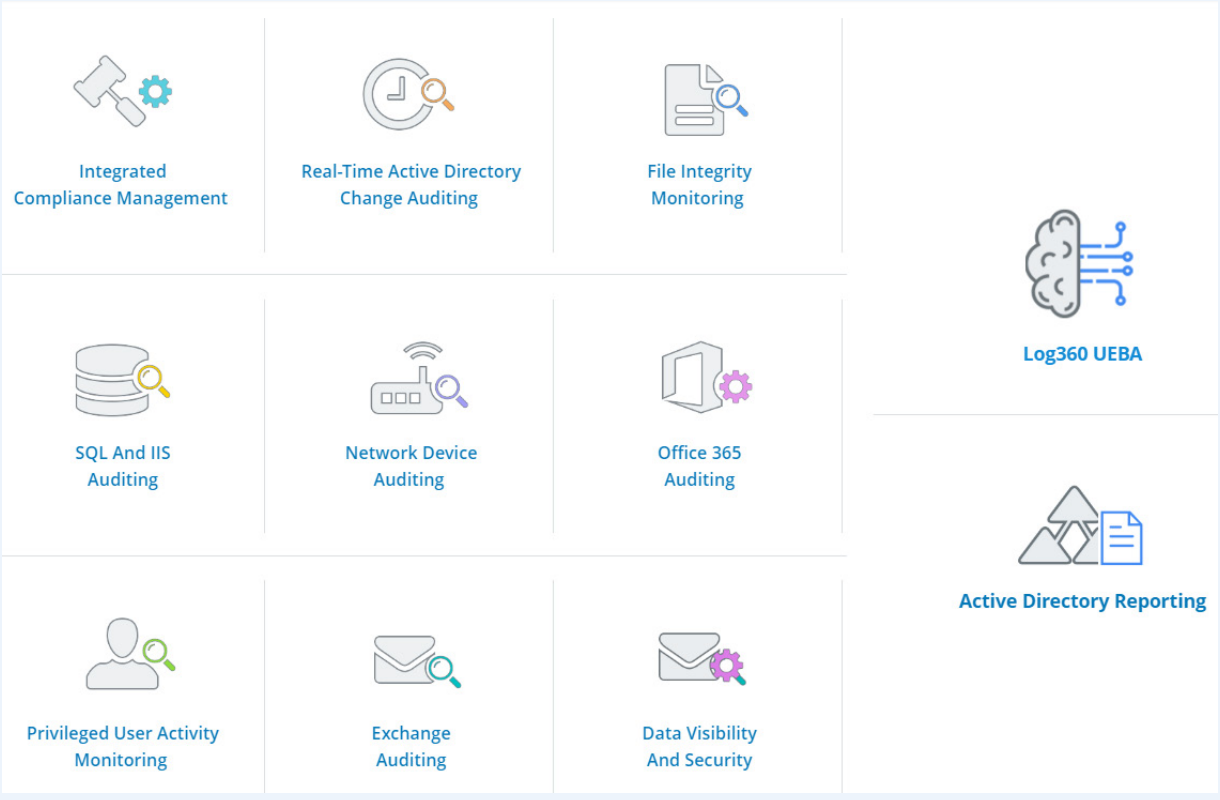

*Firewall log management*



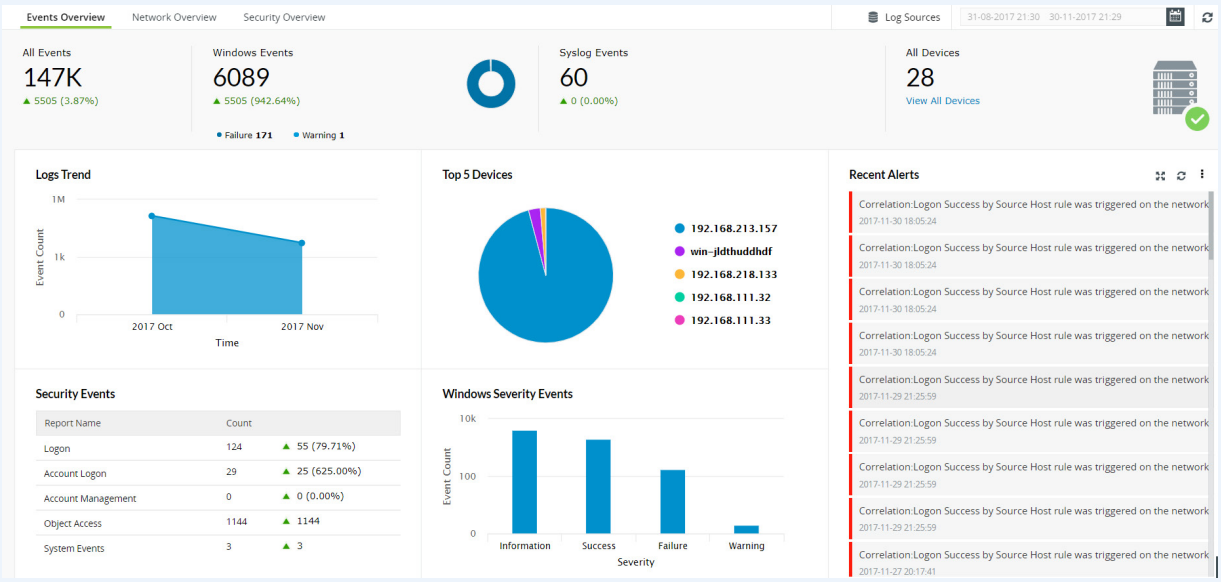

*Firewall log management*

## Log360

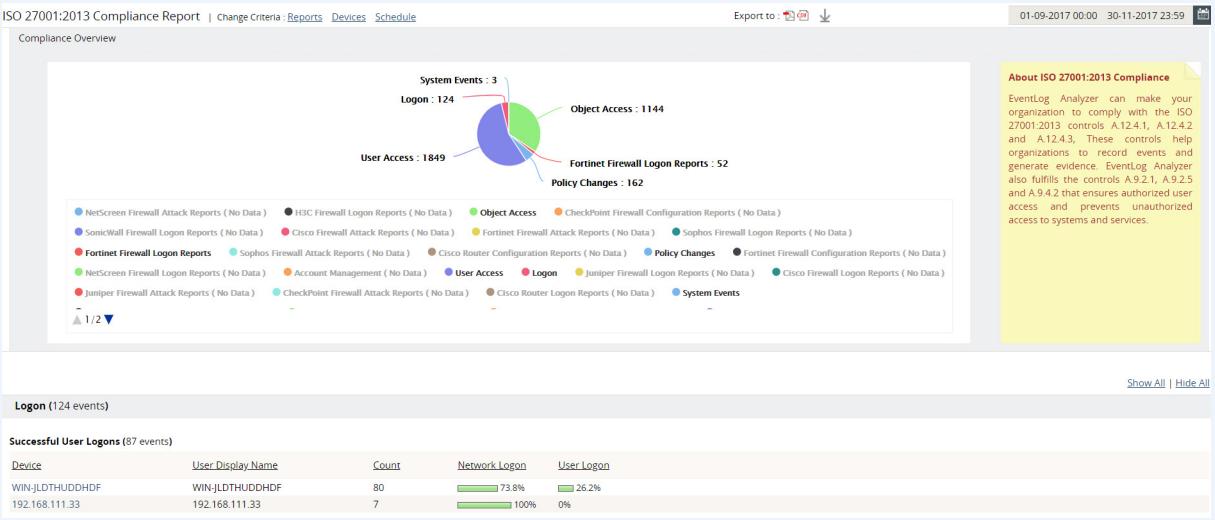
- Audit the changes and activities on Active Directory, file servers, network devices, servers, applications, databases, workstations, Microsoft 365, Exchange, AWS, Azure, etc., which serves as a evidence against the implemented controls and also to evaluate the effectiveness and to identify opportunities for improvement. It provides reporting on ISO 27001 controls as well by default.




*Log 360: Comprehensive SIEM solution*



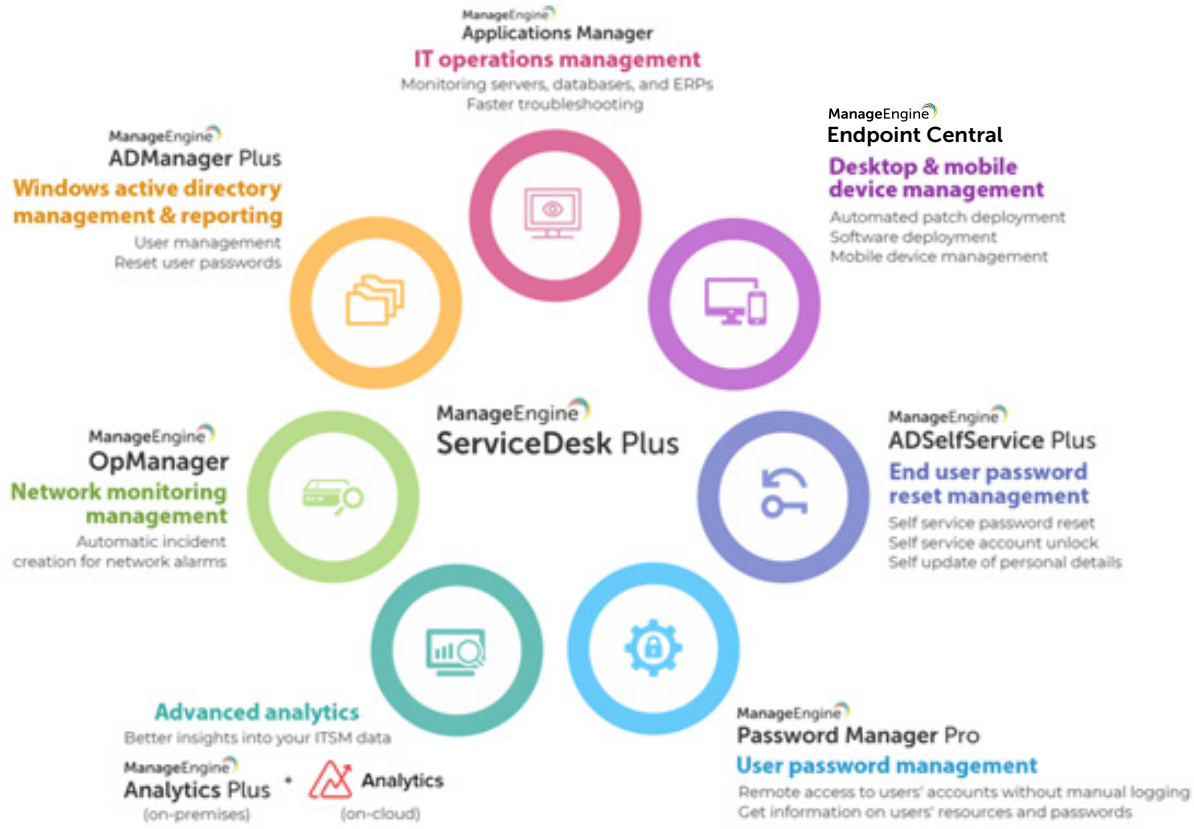

*Events overview*




*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

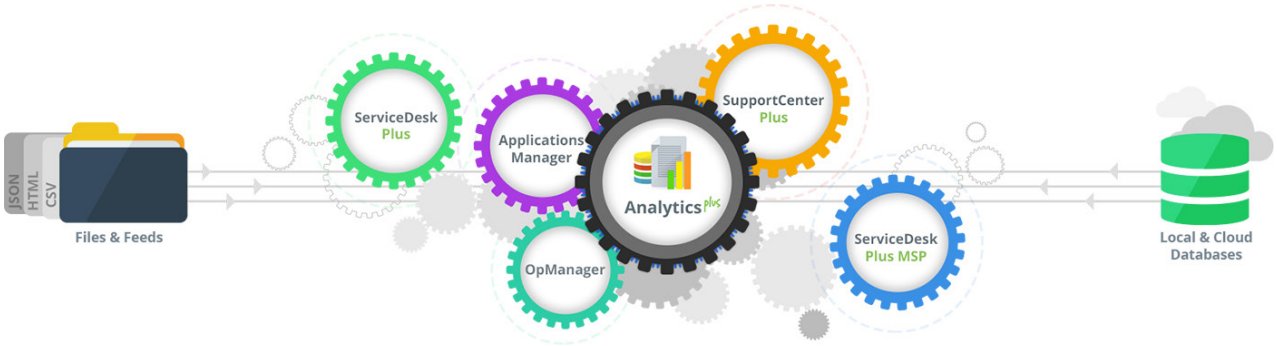
# 9.4 Service reporting

### 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*

ManageEngine

# Take control of your IT.

Monitor, manage, and secure your digital enterprise with ManageEngine.

## Unified 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 and security

- 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
- Endpoint data loss prevention

## IT operations management and observability

- 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—over 60 products—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.

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