

NEWSLETTER



Welcome to ME by Nettobe!

It's with great excitement that we launch this very first edition of our ME by Nettobe Newsletter — your bi-weekly source for the latest news, updates, and insights on all things ManageEngine in Mauritius.

Here, you'll find product updates, tips and best practices, special promotions, and event announcements — all curated to help you get the most out of your ManageEngine solutions. Whether you're an IT professional, a business leader, or simply curious about how ManageEngine can transform your operations, this is the place to stay informed and inspired.

Thank you for joining our growing community. Let's keep learning, improving, and building better IT management together!

Warm regards,
Joshua Matthew Prosper
Channel Manager
NettobeGroup

Official **ManageEngine Distributor**
for Mauritius

matthew.prosper@net2be.com
+230 5254 8544

What to Expect in Every Edition

In each bi-weekly issue of the ME by Nettobe Newsletter, you'll find:

- **Product Updates & New Features** – Stay ahead with the latest enhancements across the ManageEngine suite.
- **Tips & Best Practices** – Practical advice to optimise performance, security, and user experience.
- **Upcoming Events & Training** – Be the first to know about webinars, workshops, and special offers.
- **Local Success Stories** – Learn how Mauritian organisations are leveraging ManageEngine to solve real-world challenges.
- **Promotions & Special Deals** – Exclusive offers available only through Nettobe's official channel.

Our goal is to keep you informed, empowered, and ready to make the most of your **ManageEngine** investment.

Written By: Bryan Pascal

Strategic Cloud Monitoring: Safeguarding Performance, Security, and Compliance

The advent of cloud services has brought about a significant transformation in how organizations manage and deploy their IT infrastructure. Traditional on-premises systems, which once required extensive physical resources and constant manual oversight, are increasingly being replaced by cloud-based solutions. These modern technologies offer scalability, flexibility, and cost-efficiency that were previously difficult to achieve. However, as the reliance on cloud infrastructure grows, so does the need for robust and continuous monitoring. Monitoring cloud environments is now not just a technical necessity but a strategic imperative for ensuring performance, data integrity, and privacy.

The Rise of Cloud Services

Over the past decade, cloud computing has emerged as a dominant force in the IT sector. Organizations across all industries are leveraging cloud platforms—such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)—to host applications, store data, and run mission-critical operations. The benefits are numerous: businesses can scale resources on demand, reduce capital expenditures on hardware, and streamline IT management. Cloud services also support remote access, collaboration, and business continuity planning.

Despite these benefits, moving to the cloud introduces a set of challenges. As cloud infrastructures become more complex and diverse, organizations often struggle with visibility, control, and security.



Public Profile

Bryan Pascal

Current Role: Head of Technical Strategy at Nettobe Group.

Professional Focus: Drives technical adoption and strategy overseeing the integration and alignment of technological initiatives with the company's broader strategic goals.

hts@net2be.com | 5255 3306

Ensuring optimal performance while maintaining compliance with data protection laws is an ongoing concern. This makes real-time monitoring an essential component of any successful cloud strategy.

While cloud services bring unprecedented agility and efficiency, they also expose organisations to new risks. Data breaches, unauthorised access, service disruptions, and regulatory non-compliance are all potential threats in a cloud setting. Without adequate monitoring tools, these risks can go unnoticed until significant damage has occurred.

The Importance of Monitoring Cloud Environments

Monitoring cloud environments enables organisations to keep a vigilant eye on their systems. It helps detect performance bottlenecks, unauthorised activities, and resource inefficiencies. Additionally, it plays a crucial role in maintaining service-level agreements (SLAs) and improving customer satisfaction. Monitoring tools provide real-time insights into application health, infrastructure performance, and user activity—ensuring that IT teams can respond proactively to issues before they escalate.

ManageEngine Cloud Monitoring: A Comprehensive Solution

One of the leading solutions in the cloud monitoring space is ManageEngine Cloud Monitoring. Designed to meet the growing demands of modern IT environments, this software offers an all-in-one platform for observing, analyzing, and optimizing cloud services. Whether organizations use public, private, or hybrid cloud models, ManageEngine provides deep visibility and actionable intelligence.

Strategic Cloud Monitoring: Safeguarding Performance, Security, and Compliance

Key Features of ManageEngine Cloud Monitoring

ManageEngine Cloud Monitoring includes a robust set of features that cater to the diverse needs of IT operations:

- **1. Real-Time Monitoring** – Continuously tracks the health and performance of cloud resources, enabling instant detection of problems and facilitating swift resolution.
- **2. Comprehensive Performance Metrics** – Offers detailed analytics on applications, servers, and network components, ensuring that end-users receive high-performance and uninterrupted service.
- **3. Automated Alerts and Notifications** – Sends timely alerts about unusual activities, potential threats, or performance degradation, allowing IT teams to act before users are impacted.
- **4. Compliance and Audit Tracking** – Assists in meeting regulatory requirements by providing tools for tracking access controls, user actions, and data usage policies.
- **5. Custom Dashboards and Reports** – Enables IT administrators to create tailored views of their cloud environment and generate reports for internal audits or compliance purposes.

Conclusion

In today's fast-paced digital landscape, the shift to cloud-based systems is not just a trend—it's a fundamental evolution in IT. However, the benefits of cloud computing can only be fully realized if supported by effective monitoring practices. Solutions like ManageEngine Cloud Monitoring empower organizations to stay ahead of performance issues, security threats, and compliance challenges. With real-time visibility and intelligent alerting, businesses can ensure the integrity, efficiency, and resilience of their cloud infrastructure. As cloud technologies continue to grow in complexity and importance, investing in robust monitoring tools is no longer optional—it is essential.

Implementation of ManageEngine Endpoint Central: A Strategic Solution for Endpoint Management

As part of my role within a company that distributes ManageEngine products, I had the opportunity to lead the implementation of Endpoint Central for a client facing significant challenges in managing its IT assets. This hands-on experience confirmed my belief that Endpoint Central is far more than just a management tool — it is a key driver of performance, security, and operational efficiency for any organization.

The client, a large multi-site enterprise operating across several African countries, managed a diverse fleet of IT equipment, including desktops, laptops, tablets, and smartphones. With part of the workforce operating remotely, software updates were inconsistent, complicating both security and maintenance.

The decentralized nature of IT management across five distant sites made it difficult to maintain centralized control over software installations. Without a unified platform, the IT team spent an excessive amount of time manually tracking incidents and deploying applications. This situation not only increased security risks but also slowed down the responsiveness of technical support. The client therefore needed a solution capable of centralizing and securing the management of its IT infrastructure.



Public Profile

Berenice Amani

Current Role: ManageEngine System Integrator & Support Engineer at Nettebe Group.

Professional Focus: End-to-end implementation, configuration, and support of ManageEngine products, ensuring seamless integration into clients' IT environments and delivering maximum operational value.



Implementation of ManageEngine Endpoint Central: A Strategic Solution for Endpoint Management

In response to this need, we proposed the implementation of ManageEngine Endpoint Central, a Unified Endpoint Management (UEM) solution designed to centralize the administration of all devices. From the early stages of deployment, the solution stood out for its seamless integration and ease of use. The entire IT fleet was connected to the management console within just a few days.

We activated several key features:

- **Automated patch management**, enabling critical updates to be deployed across all devices without manual intervention
- **Remote software deployment**, making it easy to install business applications without the need for onsite visits
- **Remote desktop control**, which significantly improved user support, particularly for remote employees
- **Mobile Device Management (MDM)**, used to configure and secure mobile devices across the organisation
- **Automated compliance reports**, providing clear and continuous visibility into the health of the IT environment

After just a few weeks, the benefits were clearly visible:

- A significant reduction in incidents related to software non-compliance
- Substantial time savings for the IT team
- Lower cybersecurity risks through improved update management
- Faster and more efficient support, thanks to integrated remote access tools

This experience demonstrated how effectively Endpoint Central addresses the practical needs of modern businesses. It facilitates efficient endpoint management, bolsters cybersecurity, standardises IT processes, and improves internal service quality.

Having personally overseen its implementation on the ground, I strongly recommend **ManageEngine Endpoint Central** to any organisation looking to modernize and secure the management of its IT assets.

How ManageEngine OpManager Helps Organizations: Insights from the Field

As organisations continue to embrace digital transformation, the complexity of their IT infrastructure grows. Keeping networks optimised, secure, and resilient becomes a challenge, one that demands intelligent monitoring and automation tools. From my experience as an IT Support Engineer at NETTOBE GROUP, and having actively participated in deployments across various Mauritian organisations, I've seen firsthand how ManageEngine OpManager transforms network management and IT operations.

Real-Time Visibility into Network Health

With OpManager, businesses gain a centralised dashboard that provides real-time insights into routers, switches, firewalls, servers, and virtual machines. At client sites, I've deployed network monitoring tools that reduced average downtime incidents by over 40%, simply by proactively identifying bottlenecks and failed devices before users even notice issues.

Early Detection Reduces Business Disruption

Downtime equals lost revenue. One banking client we supported experienced recurring disruptions due to unmanaged infrastructure faults. After integrating OpManager, which provides threshold-based alerts and automated root-cause analysis, we observed a 60% reduction in incident response time. It helped their internal IT team stay ahead of outages, ensuring smoother operations.



Public Profile

Orychel Goune

Current Role: ManageEngine System Integrator & Support Engineer

Professional Focus: Deploy, configure, and maintain ManageEngine solutions across client environments with a strong emphasis on performance optimisation, security, and scalability.

Simplified Multi-Vendor Device Monitoring

In real-world environments, networks consist of devices from various vendors Cisco, HP, Fortinet, Barracuda, etc. OpManager supports out of the box monitoring for 2,000+ device types, and I've successfully integrated it with devices such as Barracuda NextGen Firewalls, Aruba Access Points, and VMware virtual machines during client rollouts. This eliminates the need for multiple siloed tools, streamlining operations and reducing software costs.

Intelligent Alerts and Automation

Manual monitoring leads to missed alerts. With OpManager's intelligent alerting and workflow automation, we configured smart alerts for high CPU usage, link failures, and security anomalies. One of our clients saved nearly 80 hours/month in manual troubleshooting by automating tasks like service restarts and SNMP trap-based notifications.

Scalability for Future Growth

Organisations that plan to grow need a tool that scales. Whether it's a small legal firm or a large electricity board (like CEB Mauritius, where I handled Barracuda ESG deployment), OpManager's modular architecture allows for gradual feature expansion, including network configuration management (NCM), NetFlow traffic analysis, and advanced reporting tailored to evolving business needs.

How ManageEngine OpManager Helps Organizations: Insights from the Field

Secure and Customisable Dashboards

Security and visibility go hand in hand. With role-based access and customisable dashboards, different departments or branch offices can access relevant metrics without compromising sensitive infrastructure data. During our implementation at Sicom Mauritius, we utilised this feature to differentiate operational views for Helpdesk staff and IT managers, enhancing accountability and transparency.

Conclusion

ManageEngine OpManager is more than a monitoring tool. It's a proactive infrastructure management solution that supports business continuity and operational efficiency. From my hands-on experience across various sectors in Mauritius, I can confidently say that integrating OpManager into an organisation's IT ecosystem significantly improves performance, reduces downtime, and empowers IT teams to focus on innovation instead of firefighting.

For businesses aiming to optimise their network infrastructure with minimal complexity, OpManager is an investment that pays for itself in time saved, issues prevented, and peace of mind gained.

Active Directory Management: The Hidden Factor Behind Business Efficiency in Mauritius

When most professionals think about ways that business can grow in Mauritius, they often picture new market development, innovative products or even stronger sales teams. There's often an underestimated factor that keep everything in the business running smoothly - How the organisation successfully manages its users, permissions and IT security.

In almost every medium to large enterprises here Mauritius, Active Directory plays a major role. It is the central system that decides who can access what, when, and how. When this is all managed, everything run smoothly — employees log in, access to files, and using resources without a hitch. Unfortunately, when AD is messy or even poorly maintained, the side effects are almost immediate:

- Delays in onboarding for new hires.
- Frustrating password issues.
- Security risks from old accounts still being activated.
- Compliance gaps that can cost your business.

That's exactly where ManageEngine Ad Manager Plus change the whole game drastically.



Public Profile

Julien Christophe

Current Role: Sales Executive at Nettobe Group

Professional Focus: looks after sales and sales activities for ManageEngine with endusers and partners

julien.christophe@net2be.com
+230 5254 7872



Why Mauritian Business Struggle With AD ?

From Financial Institutions in Port-Louis to Hospitality Groups in Grand Baie, Many IT Teams nowadays face the same challenges:

- Manual Processes : Creating, Modifying, or deleting accounts one by one.
- Poor Visibility: Not knowing which users have unnecessary access.
- Audit Headaches: Struggling to produce accurate reports for compliance.
- Security blinds sets: Dormant accounts that can be exploited.

In fact, based to our internal sources, almost all Mauritian companies we engaged this year so far, have reported at least one dormant user account is still active after the employee had left. This is because there is a lack of automation, especially in a high busy work environment, these are not just “IT issues” but can also be characterised as business risks, as from there are delays in project s, employees are frustrated, and even this can cause customers' trust can erode.

AdManager Plus: From It Burdens to Business Advantages

AdManager Plus from ManageEngine is designed specifically to take the complexity out of the Active Directory Management . Here's to convert a technical tasks into a competitive advantage:

- **One-Click User Management:** Create, update, or disable multiple user accounts in one go — perfect for fast onboarding and secure off-boarding processes.
- **Automated Workflows:** Set up pre-defined processes so routine tasks happen without IT bottlenecks.
- **Custom Reports in Seconds:** Instantly see who has access to what, which accounts are inactive, and where risks lie.
- **Delegated Administration:** Give department heads the power to manage their own teams' accounts — without giving them full IT control.
- **Compliance Mde Easy:** Generate audit-ready reports for GDPR,ISO, or Internal governance in just a few clicks.

Why Now Is The Right Time To Consider AdManager Plus

From a sales Standpoint, the Mauritian market is at a turning point, our data shows that:

- 80% of companies we spoke to in the last [Y months] are still managing AD accounts manually
- 63% reported recent security or compliance concerns tied to account mismanagement
- Businesses using automation saved an average of 3.2 hrs per week in IT workloads.

This means that a significant amount of large organisations are still facing issues related to the management of the AD, problems that matter of fact, AdManager Plus can solve immediately.

For us, this is not just an IT conversation — it's an opportunity to solve a pain point that is costing companies money right now.

Three Triggers That Make Prospects Ready to Buy

From the sales side, we've identified three scenarios where Mauritian companies are most open to implementing ADManager Plus:

- **Rapid Growth or Seasonal Hiring**

Companies are adding large numbers of employees — especially in retail, hospitality, or finance — struggle with fast onboarding and secure off-boarding.

- **Upcoming Compliance Audits**

Businesses preparing for GDPR, ISO, or sector-specific audits are looking for tools that deliver instant, audit-ready reports.

- **Security Incidents or Breaches**

When a dormant or mismanaged account is exploited, urgency skyrockets. Companies want a fix fast.

Closing Thought

The Mauritian market is full of companies quietly struggling with AD management. Each one represents a potential deal for us — not because they want ADManager Plus, but because they need it.

If we position ourselves with the right timing, the right pain points, and the right proof, ADManager Plus can become one of our strongest revenue drivers this year.

ManageEngine

Special ITCON25MAU Promo

Get an additional 5% discount on your purchase of any ManageEngine license — license only — as part of our ITCON25 Mauritius special offer!

Conditions apply. Offer valid for a limited time only.



ITCON 2025 – Mauritius by ManageEngine

ITCON 2025 really was something special for our Mauritian IT community. It wasn't just another event; it was a gathering of brilliant minds, innovators, and decision-makers who came to see, learn, and explore the latest in IT management, cybersecurity, and digital transformation.

A Real Collaboration—Global Meets Local

This year, the ManageEngine engineers themselves were here, in person, sharing their deep product knowledge and global expertise right on our shores. As Nettobe Group, the official distributor of ManageEngine for Mauritius, we were proud to carry the local side of the work—from the big logistics and coordination to the small details like registration, welcoming everyone, and making sure post-event follow-ups were done.

Honestly, the way it all came together showed me again that when you mix global expertise with local dedication, you get something powerful.

Some Highlights Worth Remembering

- **Tech Sessions That Made Sense**—We didn't just hear about Endpoint Central, AD360, OpManager, and Analytics Plus—we saw them in action, in live demos that made it real.
- **Smooth Event Flow**—From check-in to closing remarks, the day ran well. Our team was everywhere, quietly making sure things worked without fuss.
- **Connections That Matter**—We saw people from government, finance, healthcare, and education having the right conversations, the kind that spark real projects.

Why This Matters for Mauritius

It's simple: our IT leaders had access to international expertise without the cost or hassle of leaving the country. We showed that Nettobe's role isn't just selling licenses—it's bridging the global and the local, making sure world-class tech is understood, implemented, and supported right here in Mauritius.

Looking Forward

ITCON 2025 wasn't just a conference; it was a signal—that Mauritius is ready for advanced, integrated IT management solutions. And we, together with ManageEngine, are ready to deliver them.

From me personally—thank you.

To our **resellers**, your trust in bringing ManageEngine to your clients is the reason this ecosystem works. To our **transactional partners**, your behind-the-scenes role might not always be on the stage, but without you, events like this wouldn't even happen.

To **our customers and attendees**, thank you for your time, attention, and feedback—you make this worth doing.

The journey for ManageEngine in Mauritius is still just starting... and honestly, I think the best is still ahead of us.

— Matthew Prosper

ITCON 2025 IN IMAGE



Turning Chaos into Clarity with Effective Incident Communication

When technology hiccups, whether it's a small glitch or a full system meltdown, how you communicate it is almost as important as fixing it. That's where incident communication, the process of delivering timely, clear, and consistent updates to everyone involved, from users and technicians to leadership, comes in. Every stage of an incident, from logging the initial ticket to sharing progress updates, confirming resolution, and reviewing the root cause, requires thoughtful communication. And this's exactly where ITSM solutions step in.

Designed to orchestrate the incident communication process, ITSM platforms reduce ambiguity and manual effort by automating alerts and notifications at key stages based on predefined rules and incident life cycle stages. With AI in the mix, these systems can even generate conversation summaries and post-incident reports, making communication more efficient and actionable. In this article, let's look at how structured, strategic communication can reduce chaos, build trust, and streamline response during IT incidents.

Why is incident communication more than just an FYI?

- **It calms the chaos.** Quick and clear communication can stop people from panicking or spinning their wheels trying to troubleshoot the issue themselves.
- **It builds trust.** Even if you don't have all the answers yet, letting people know you're aware of the issue shows accountability and helps keep people in the loop.
- **It reduces the IT service desk load.** When users are updated proactively, they're less likely to raise tickets or call support to ask what's going on. That frees up the IT service desk team to focus on fixing the issue instead of repeating the same message a hundred times.
- **It helps the response team stay aligned.** Communication keeps the internal teams aligned, especially when multiple departments are working together to resolve an incident.



Public Profile

Nii Nortey

Current Role: ManageEngine System Integrator & Support Engineer

Professional Focus: Deploy, configure, and maintain ManageEngine solutions across client environments with a strong emphasis on performance optimisation, security, and scalability.

How to Have an Effective Incident Communication Process

Ensuring that the right information reaches the right people without delay or misinterpretation is key. The way we communicate needs to adapt to the situation, whether it's a minor incident impacting a few users or a major outage affecting the entire organization. Adjusting our approach accordingly ensures stakeholders receive clear and meaningful updates.

For example, say Sarah creates an incident ticket via the self-service portal to report that her email client is crashing repeatedly. This initial contact sets in motion a structured communication framework embedded within the ITSM solution:

- Upon submission, the ITSM solution can promptly send an automated initial notification that serves to confirm receipt of her ticket and includes the incident number (for example, #INC35791). It also provides a direct link to a relevant knowledge base article on troubleshooting email client issues, if any, enabling Sarah to explore potential self-help solutions while awaiting further action.
- Subsequently, when a technician is assigned or reassigned to the incident ticket, they automatically receive an update about it along with other information like the incident number, or a direct link to the ticket.

- As the assigned technician undertakes diagnostic and resolution efforts, the incident's status within the ITSM system undergoes corresponding updates. Each significant change in status (for example, In Progress, Awaiting Approval, Resolved), or any escalation of the incident to a specialized team, such as the Exchange team for more intricate email-related issues, automatically triggers a notification to Sarah. This keeps her informed of the incident's trajectory and the actions being taken.
- In scenarios where an incident approaches an SLA breach, the system can automatically send out escalation notifications to relevant support teams and the manager. This proactive escalation prompts timely intervention.
- If the resolution requires any approval, automated approval notification including the link to approval is sent to the relevant approval manager. This ensures a streamlined approval process, mitigating potential bottlenecks, and facilitating the timely implementation of the required actions.
- Upon successful resolution of the email client issue, the technician records the resolution details within the incident ticket. This action automatically triggers a formal resolution confirmation email to Sarah. This communication includes a concise summary of the implemented corrective measures and a hyperlink to a satisfaction survey for Sarah to provide feedback on her support experience.
- If the issue reoccurs after the incident has been resolved and Sarah reopens the incident, the technician will be notified and will follow the resolution process again until the incident is closed.

While that works well for low-severity incidents, broader disruptions require a different level of communication. Let's say the digital landscape starts to crumble. The alert from the monitoring tool raises an incident ticket. It's not just Sarah's email acting up, but a widespread outage affecting multiple users or critical services; the communication game changes significantly. It's no longer about individual ticket updates; it's about orchestrated, multi-channel communication that keeps a larger audience informed and manages expectations effectively. In such scenarios, the incident communication unfolds in four parts: first contact, regular updates during the incident, resolution, and post-incident review.

1. First contact: Getting the word out quickly and clearly

When a major incident strikes, the initial communication is critical. It's vital to acknowledge the issue swiftly and provide enough information to give stakeholders a heads-up. Leveraging the broadcast notification feature in your ITSM tool for an initial email is a standard best practice for reaching a wide audience quickly. Expanding on that, using a telephony application to distribute an SMS to relevant groups adds another layer of urgency and ensures visibility for those who need immediate awareness, even if they aren't constantly monitoring their email. You can display an announcement banner in the self-service portal to avoid users reporting multiple incident tickets. This initial contact should aim to answer:

- **What happened?** A concise summary of the situation.
- **Who is affected?** Be specific about the services, systems, or user groups impacted.
- **What are the next steps?** Let people know that the incident response team is engaged and working on it. Inform them when they can expect the next update.
- **Where can they get more information?** Direct them to a designated channel (status page, incident ticket, announcement banners, etc.).

Example: MAJOR INCIDENT: Core services (for example, Apps, Website) are currently down, impacting all users. Our team is working to restore. Expect the next update in 30 minutes.

2. Regular updates during the incident: Keeping everyone in the loop

Provide updates on progress, changes, and timelines.

- Set a cadence for updates based on the severity and pace of the incident. Even if there's no significant change, a "still investigating" update is better than nothing. Include workarounds if available.
- If changes to an IT system or application are required to resolve the issue, the ITSM tool should notify stakeholders with the change ticket details and clearly communicate the potential impact once the ticket is created.
- Stick to the communication channels established in the first contact to avoid confusion.

3. Resolution: Announcing the all-clear

The resolution announcement is the moment everyone has been waiting for. This communication should include:

- Clearly state that the issue is resolved and the impacted services are back to normal. Indicate when the services were restored.
- Briefly explain what actions were taken to resolve the incident.
- If there are any temporary limitations that the users should be aware of post-resolution, mention them.

4. Post-incident review: Learning and improving for the future

The post-incident review is a key moment to learn, reflect, and improve. The communication around this phase involves:

- Informing stakeholders that a post-incident review is being done.
- Once the post-incident review is complete, sharing a high-level summary of the root cause, learnings, and preventive measures to prevent such issues in the future.

If the issue is recurring and a problem ticket has been created to address it, the ITSM tool should notify the relevant stakeholders with the problem ticket details.

Tips to Make Incident Communication Smoother

- Use predefined templates for different incident types and severities. This ensures consistent, clear, and timely information for all stakeholders.
- Segment audiences (end users, IT, leadership) and tailor messages to their specific informational needs.



Why Use ServiceDesk Plus For Incident Communication

ServiceDesk Plus empowers IT teams to deliver effective incident communication through a suite of built-in features. Automated notification rules ensure that both users and technicians receive timely updates based on changes in ticket status throughout the incident life cycle. Customizable email templates promote consistency across all communication streams.

In the event of major incidents, ServiceDesk Plus ensures effective communication through multiple channels, including email, SMS, push message, Microsoft Teams, and Slack. This enables IT teams to deliver timely updates to users through their preferred communication mode. The portal announcement feature keeps users informed about ongoing disruptions and helps reduce duplicate tickets. The incident workflow capabilities enable notifications to be sent based on specific conditions. Custom functions, on the other hand, automate actions such as creating incident response teams in collaboration tools, sending targeted updates, and initiating bridge calls when multiple teams need to work together. ServiceDesk Plus provides both proactive and reactive notifications for SLA breaches to ensure timely attention and resolution.

The AI assistant, Zia, which is powered by ChatGPT, analyzes incident data to generate concise summaries for stakeholders, post-incident reviews with insights, and proactive alerts based on recurring patterns. It performs root cause analysis to prevent future issues. Following incident resolution, post-incident surveys facilitate the collection of user feedback, enabling continuous service improvement. By using this mix of automation, AI, and communication channels, IT service desk teams can focus on fixing issues while users stay informed.

Want to take control of your incident narrative? ServiceDesk Plus automates proactive updates, real-time connections, and insightful reviews. Experience the ease— request your free personalized demo today!

ManageEngine
**Bringing
IT together**



Our Social Channels

Join us on WhatsApp - ManageEngine by Nettobe, LinkedIn, Facebook, and YouTube, Including our Talkshow Net2Talks – all by Nettobe Group.

CLICK ON THE ICON TO JOIN US

