ManageEngine
DDI Central

ManageEngine
DDI Central

A Single point of administration for your three core services

Modern organization are now stepping forward to adapt to the digital transformation of their network management by implementing different strategies, tools, and security measures. Their primary goal is to expand their network across different branches and location points for both clients and users to access them effectively without compromises, and increase productivity of network services by enabling automation, security policies, configurations and more.

Network admins of the organizations would find it tedious to manually monitor and manage all the devices, policies and configurations for each client's devices, and each user's role in the organization. Plus, switching between individual tools for each service management also be time consuming and less-efficient.

Solution

ManageEngine DDI Central solves the problem for network admins by offering a unified platform comprising DNS, DHCP, and IPAM—the three core services in a single point for simplified and easy access of monitoring and management. Security configurations and policies for different devices and different network segments can be applied from the single page.

Network admin can be hassle-free with network resource management and improve the overall efficiency and productivity with the help of policy-driven automation, scheduled DNS and DHCP tasks, monitoring IP utilization, allocation of IP resources to selective clients,

What you can do with DDI Central?

DNS-DHCP service provider

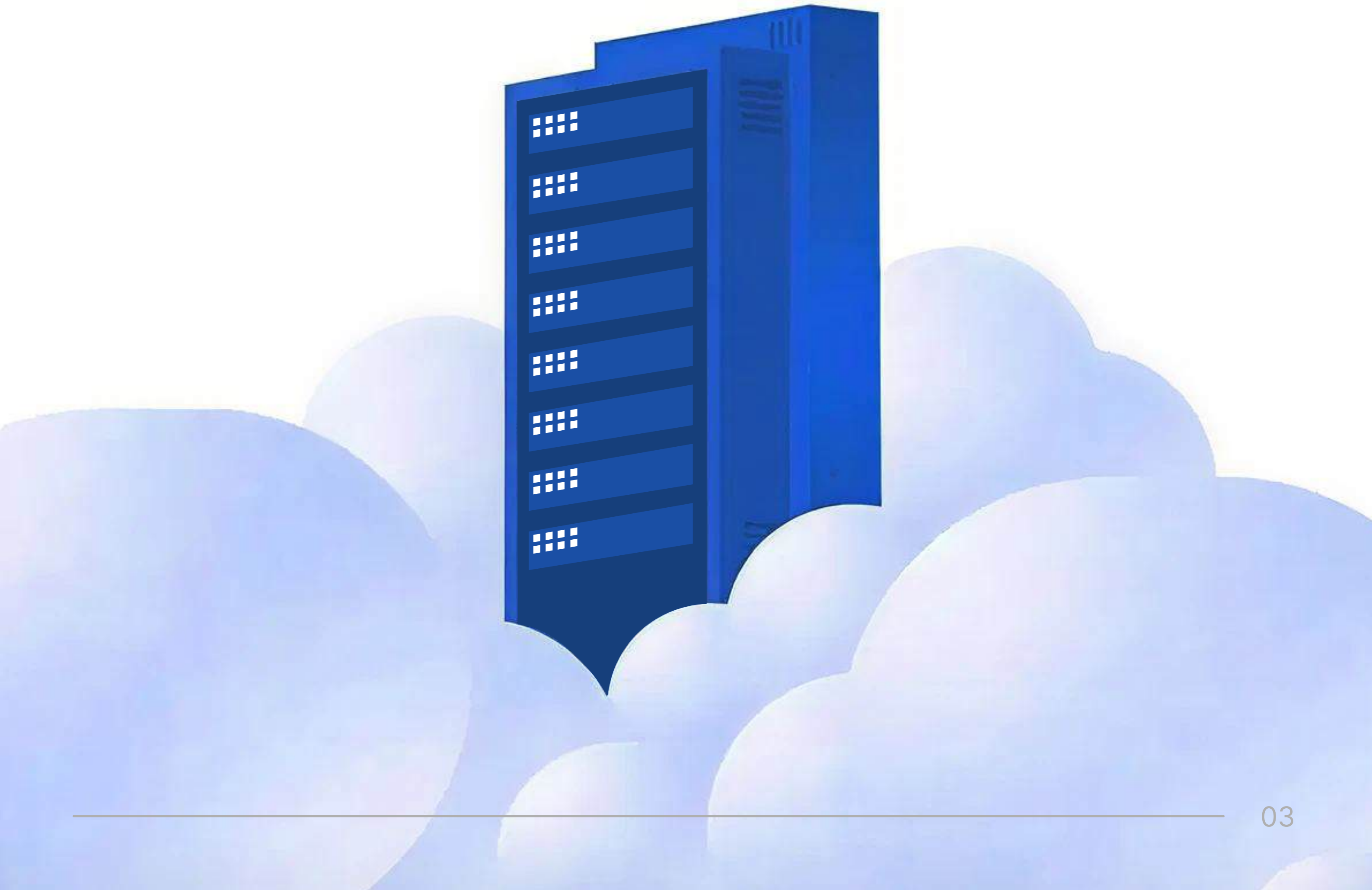
- ✓ Within each cluster, you get DNS management, DHCP management, and IP address inventory/space, all of which can be monitored and managed individually—eliminating the need to switch between separate tools for each service.

Multi-tenant Architecture

- ✓ DDI Central allows network admins to add individual servers from multiple organizational sites, each with their own services and configurations, as separate clusters. All branch office and site clusters can then be discovered and managed through the application's centralized platform.

Cross-platform integrator

- ✓ DDI Central integrates with Linux (ISC BIND and DHCPd) and Windows DNS/DHCP servers. Cluster configurations, features, and policies are platform-specific and optimized separately for Linux and Windows deployments.



DNS management

Simplified DNS server setup

- ✓ Configure and set up authoritative and recursive DNS servers, or seamlessly allow DDI to discover existing servers and their configurations.
- ✓ Monitor network, IP, CPU, memory, and disk utilization of your DNS servers from a single dashboard.

DNS zone management

- ✓ Add, update, or delete the zone file data of your domain's DNS records for consistent zone management.
- ✓ Create new authoritative zones or import existing ones.
- ✓ Create new DNS records or import existing records.

Dynamic DNS (DDNS) with Transaction Signature (TSIG)

- ✓ Maintain updated zone files for dynamically changing IPs through secure automation.
- ✓ Ensure consistent network services and availability for clients through automated IP updates in DNS zones.

Query response analytics

- ✓ Gain real-time insights into DNS network traffic, including total queries, queries per second, and more.
- ✓ View query analytics for blocked domains within your internal DNS infrastructure.

Rate limiting policies

- ✓ Prevent your DNS servers from abuse and attacks by implementing rate-limiting policies.
- ✓ Mitigate the total number of responses for each DNS request to prevent server downtime and network disruption.

DNS firewall based blocking

- ✓ Enhance your DNS network security by blocking unwanted or malicious domains using DNS firewall policies.
- ✓ Protect your DNS infrastructure from unauthorized access and potential cyberthreats.

DNS security management

DNS threat intelligence

- Block malicious domains in your network by integrating threat feeds from ManageEngine CloudDNS, top cybersecurity vendors, or custom STIX/TAXII sources.
- Use reputational scores for effective DNS layer defense.

Anomaly detection

- Detect domain generation algorithm (DGA) domains and suspicious TLD patterns.
- Identify DNS tunneling, Windows/DNS policy abuse, and DHCP anomalies in your network.

DNS over TLS (DoT)/DNS over HTTPS (DoH)

- Encrypt DNS traffic with DoT and DoH to protect user privacy and ensure data integrity for both enterprise networks and privacy-focused environments.

DNS/Domain view

- Customize DNS resolution for specific departments and clients in your network through DNS/Domain views.
- Protect your network's confidential information from unauthorized access while ensuring consistent service.

DNS detection and response (DDR)

- Quarantine suspicious IPs and subnets in real time by blocking DNS queries and DHCP leases for restricted clients.
- Prevent cyberthreats at both the DNS and DHCP levels in your network.

Response rate limiting (RRL)

- Protect servers from abuse and query overload by controlling response rates through RRL.
- Allow admins to configure the total number of responses per DNS request, providing robust control over DNS resolution.

Response Policy Zones (RPZ)

- Prevent malware communications and access to malicious domains using DNS firewall policies based on RPZ domain analysis.
- Implement proactive security measures to block the resolution of undesirable domains and malware entries.

DNSSEC with TSIG

- Mitigate the risks of cache poisoning and DNS amplification attacks by verifying DNS responses using cryptographic signatures.
- Validate responses for different user groups and network segments within your organization.

DHCP management

Simplified DHCP server setup

- Set up new DHCP servers manually or discover existing servers along with their configurations and assets.
- Monitor your DHCP servers' network, IP, CPU, memory, and disk utilization from a single dashboard.

DHCP fingerprinting

- Customize IP allocation for specific clients by categorizing them using DHCP Fingerprinting based on their MAC addresses.
- Identify, categorize, and control different types of devices connecting to your network.
- Implement tailored policies for specific clients using client classes.

DHCP reservation

- Reserve fixed IP addresses for specific devices that require 24/7 consistent IP access.
- Ensure critical devices, such as printers, cameras, and servers, remain reliably connected to your network.

PXE boot templates

- Create templates for file deployment across your organization's devices.
- Deploy files to all devices in your organization simultaneously.

DHCP scope management

- Automate IP lease management by defining address pools within hierarchically organized DHCP scopes or network topology elements.
- Apply custom DHCP configurations across multiple IP address pools.

Rogue DHCP server detection

- Identify and troubleshoot rogue DHCP servers in real time through timely email alerts.
- Configure the schedule for email alerts and notifications to detect rogue DHCP servers.

DHCP failover management

- Switch DHCP services between servers when the primary server goes down, ensuring uninterrupted service.
- Provide consistent network availability for clients without any compromises.

DHCP MAC filtering

- Elevate network security by controlling access through MAC address filtering.
- Allow or deny devices based on their MAC addresses to prevent unauthorized network access.

Static scope monitoring

- Elevate network security by controlling access through MAC address filtering.
- Allow or deny devices based on their MAC addresses to prevent unauthorized network access.

IPAM management

SimplifieIP address space visibility DHCP server setup

- Gain a complete, centralized view of your organization’s IP address space and utilization insights.
- Maintain robust control over IP address allocation for client devices to optimize IP usage.

Lease history insights

- Track and analyze the complete DHCP lease history of your IP address space and associated devices.
- Assign specific hosts to available IP addresses manually to ensure consistent IP service.

IP-MAC Identity mapping

- Access information about user devices connected to your network.
- Analyze the IP usage of each device in your network.
- Troubleshoot network disruptions and conflicts by identifying the devices causing them.

Cloud observability

Third-party migrations

- Migrate all your cloud providers’ zones and domains—including AWS, GCP, Azure, and Cloudflare—into DDI Central for centralized management.
- Gain clear visibility of your cloud providers’ assets through the application dashboard.

Multi-vendor DNS integration

- Gain control over your entire multi-cloud environment from a single interface.
- Create, edit, and delete zones and domains across multiple cloud providers within DDI Central.
- Ensure that any changes made to zones and domains are reflected across all cloud providers through automated two-way synchronization.

Cloud native asset management

- Correlate and visualize all cloud native assets of AWS, GCP, and Azure from a centralized console for deeper insights.
- Provision new zones and domains across cloud providers directly from DDI Central—with automatic two-way synchronization to ensure changes made in DDI Central or the provider stay fully aligned.

Why choose DDI Central for network services management?

- ✓ Streamlined multi-cloud observability for hybrid infrastructures
- ✓ Simplified navigation with an intuitive UI interface
- ✓ Wide-scale remote site monitoring and management
- ✓ Centralized control of DNS, DHCP, and IP address resources
- ✓ Enhanced DNS, DHCP, and IP discovery capabilities
- ✓ Policy-driven IPv4 and IPv6 assignments
- ✓ Scheduled DNS and DHCP configurations
- ✓ Smarter administration of static or delegated scopes
- ✓ Advanced scope monitoring
- ✓ Plug-and-play deployment with automated PXE boot provisioning
- ✓ Built-in redundancy, failover, and auditing features
- ✓ Role-based access controls and REST API integration
- ✓ Detailed reporting and advanced analytics

Pricing

Professional Edition

2 Admin/Operator roles, 15 zones, and 15 subnets, 6 DNS servers. 4 DHCP servers, 3 NTP servers, 5 monitors, Anomaly Detection.

Pricing starts at

$ **3199**

Annual Subscription

Enterprise Edition

5 Admin/Operator roles, 100 zones, and 100 subnets, 15 DNS servers, 10 DHCP servers, 5 NTP servers, 15 monitors, DNS Threat Intelligence + DNS Detection and Response (DDR), Management UI Console Failover-Hot Standby Engine, Anomaly Detection.

Pricing starts at

$ **6199**

Annual Subscription

Start your 30-day, free trial now! Or request a personalized demo! to explore and understand DDI Central's features and benefits for your organization.