

H. BANAI

Long Beach, CA | (562) 316-8845 | hameedabanayee@gmail.com

LinkedIn: [linkedin.com/in/h-banai](https://www.linkedin.com/in/h-banai)

SYSTEMS ADMINISTRATOR | AZURE & MICROSOFT 365

PROFESSIONAL SUMMARY

Systems Administrator with hands-on experience supporting Microsoft and enterprise IT environments across systems administration, cloud services, endpoint management, networking, and cybersecurity. Experienced administering Microsoft 365, Microsoft Entra ID (Azure AD), Microsoft Intune, Microsoft Defender, Active Directory, Group Policy, Windows Server, SCCM/MECM, PowerShell, and Azure environments. Skilled in user and device administration, identity and access management, endpoint configuration, software deployment, patch management, network troubleshooting, vulnerability remediation, and IT infrastructure support. Additional experience with CMMC Level 2 and NIST SP 800-171 compliance initiatives. Proven ability to independently support enterprise environments and fast-paced startup operations.

TECHNICAL SKILLS

Microsoft & Cloud: Microsoft Azure • Microsoft 365 • Microsoft Entra ID (Azure AD) • Microsoft Intune • Microsoft Defender • Active Directory • Group Policy • Windows Server • PowerShell

Systems Administration: Windows 10/11 • SCCM/MECM • Endpoint Management • Device Provisioning • Software Deployment • Patch Management • User Administration • IAM • Remote Administration • Asset Management • Hardware Lifecycle Management

Networking: TCP/IP • DNS • DHCP • VLANs • VPNs • UniFi Network • Wireless Networking • Network Troubleshooting • OT/IT Networking

Security: Endpoint Security • Vulnerability Management • Wazuh SIEM • ThreatLocker • CrowdStrike Falcon • KnowBe4 • Security Monitoring • Incident Response • CMMC Level 2 • NIST SP 800-171

PROFESSIONAL EXPERIENCE

SYSTEMS ADMINISTRATOR

Space Kinetic | March 2026 – September 2026

- Administered Microsoft 365, Microsoft Entra ID, Microsoft Intune, Microsoft Defender, Windows endpoints, and enterprise IT infrastructure.

- Managed user onboarding/offboarding, account administration, device provisioning, application deployment, licensing, asset management, and hardware lifecycle activities.
- Configured and maintained Microsoft Intune policies, endpoint configurations, application deployments, and device security controls.
- Supported Microsoft Defender Vulnerability Management by reviewing endpoint exposure, software inventory, security recommendations, and remediation activities.
- Used Pulseway RMM for endpoint monitoring, remote administration, software deployment, operating system updates, patch management, and troubleshooting.
- Administered ThreatLocker Application Control, Ringfencing, Storage Control, and Elevation Control to strengthen endpoint security.
- Managed Wazuh SIEM, including security event monitoring, log review, alert investigation, and incident detection support.
- Administered UniFi Network infrastructure, including network configuration, VLANs, wireless connectivity, and network troubleshooting.
- Supported UniFi Protect, UniFi Access, and Apache Guacamole for physical security, access control, surveillance, and secure remote administration.
- Provided Tier II/III support for Microsoft 365, Windows, networking, VPN, servers, printers, endpoints, and security technologies.
- Supported CMMC Level 2 and NIST SP 800-171 initiatives through technical control documentation, audit evidence collection, security control validation, and compliance tracking using IntelliGRC.
- Designed and implemented network connectivity for Haas and Fadal CNC machines and supported IT infrastructure for manufacturing and engineering operations.
- Worked independently in a fast-paced startup environment while managing systems administration, networking, endpoint, security, and infrastructure priorities.

NETWORK ADMINISTRATOR

Behavioral Health Services | December 2024 – March 2026

- Administered Active Directory, Microsoft 365, Group Policy, Windows endpoints, and user accounts across multiple clinical facilities.
- Managed Microsoft 365 user administration, account provisioning, access management, and troubleshooting.
- Deployed operating systems, applications, software packages, and enterprise updates using Microsoft SCCM/MECM.
- Created and maintained SCCM packages, deployments, task sequences, and software distribution workflows.
- Supported Windows 10-to-Windows 11 upgrade initiatives, including hardware readiness assessments, deployment planning, and troubleshooting.
- Developed SQL queries and system reports to evaluate Windows versions, CPU compatibility, TPM, Secure Boot, RAM, and disk capacity for Windows 11 readiness.
- Supported CrowdStrike Falcon endpoint protection, vulnerability remediation, patch management, and endpoint security initiatives.
- Supported MFA implementation and identity security initiatives across enterprise users and endpoints.

- Supported SCCM, SCOM, and WSUS environments for software deployment, patch management, monitoring, and troubleshooting.
- Provided Tier II technical support for Windows, hardware, software, networking, and endpoint issues across distributed facilities.

CERTIFICATIONS

- AWS Certified Cloud Practitioner (CCP)
- CompTIA A+
- CompTIA Network+
- CompTIA IT Operations Specialist (CIOS)
- Digital Forensics Essentials (DFE)
- Ethical hacking Essentials (EHE)

CURRENTLY STUDYING

- CompTIA Security+
- SC-500

EDUCATION

Cybersecurity & Computer Networking Certificate
Long Beach City College

Master of Science
Tirana University

Bachelor of Science
Kabul University