NOVARTIS

# Assoc. Dir. DDIT ISC Identity & Access Management AD

Job ID
REQ-10090302
Окт. 27, 2026
Индия

### Сводка

We are seeking a hands-on identity security leader who:
• Has deep expertise in Active Directory Security and Microsoft Entra ID Security.
• Understands identity attack techniques and modern cyber threats.
• Has experience securing hybrid identity environments at enterprise scale.
• Can influence strategy while remaining technically credible.
• Has strong working knowledge of Microsoft 365 security technologies.
• Can engage effectively with security leadership, auditors, architects, and engineering teams.

### About the Role

**Key Responsibilities:**

- Serve as the enterprise subject matter expert and senior technical leader for Microsoft Entra ID, Hybrid Identity, and emerging Agentic Identity security.
- Own the security architecture, design, operational governance, and control framework for Microsoft Entra ID, including B2B/B2C, workload identities, and agent identities.
- Define and implement identity security standards, hardening baselines, Conditional Access controls, Zero Trust principles, and security guardrails across the identity ecosystem.
- Lead identity threat detection, protection, incident response, and recovery, including investigations involving compromised identities, risky users/sign-ins, password-spray attacks, and other identity-based threats.
- Identify and remediate identity security weaknesses and attack paths, partnering with Cyber Defense and SOC teams to strengthen detection and response capabilities.
- Govern privileged access, administrative accounts, application onboarding, provisioning, and identity lifecycle controls across large-scale enterprise environments.
- Establish and track identity security KPIs, KRIs, control effectiveness, operational health, and risk-reduction metrics, providing clear updates to security leadership.
- Provide technical leadership for complex, multi-year identity transformation initiatives, resolving architectural and operational roadblocks and driving secure, scalable solutions.
- Support internal and external audits, regulatory requirements, and compliance reviews by ensuring identity controls, evidence, and governance processes are effective and audit-ready.
- Drive operational excellence through automation, engineering discipline, continuous improvement, innovation, and adoption of emerging identity-security capabilities.

**Essential Requirement :**

- 10–12+ years of experience in enterprise Identity and Access Management, with significant hands-on responsibility for large-scale Microsoft Entra ID and hybrid identity environments.
- Deep technical expertise in Microsoft Entra ID security, including Conditional Access, External Identities, Identity Protection, Identity Governance, privileged access, application integration, and provisioning technologies such as SCIM.
- Strong knowledge of Identity Threat Detection and Response (ITDR), identity attack techniques, prevention controls, incident response, and recovery strategies.
- Proven experience designing and implementing identity controls aligned with Zero Trust architecture, security governance, and enterprise risk-management principles.
- Demonstrated ability to lead complex, multi-year identity-security programmes as a senior technical expert, resolving architectural challenges and translating strategy into practical solutions.
- Experience operating in a large, highly regulated enterprise environment, with a strong understanding of audit, compliance, control design, and evidence requirements.
- Ability to analyse identity-security data, identify risks and attack paths, define remediation priorities, and communicate technical risks clearly to senior stakeholders.
- Strong stakeholder-management and leadership skills, with the ability to engage effectively with security leadership, auditors, architects, engineering teams, Cyber Defense, and SOC functions.

**Desirable Requirement :**

- Strong working knowledge of Active Directory and hybrid identity architecture; relevant certifications such as Microsoft Identity and Access Administrator (SC-300), Microsoft Azure Security Engineer (AZ-500), CISSP, or CISM are advantageous.
- Knowledge of emerging Agentic Identity and AI-agent governance models, including lifecycle, access, security, monitoring, and accountability considerations.

**You'll receive:** You can find everything you need to know about our benefits and rewards in the Novartis Life Handbookhttps://www.novartis.com/careers/benefits-rewards

**Commitment to Diversity and Inclusion:**
Novartis is committed to building an outstanding, inclusive work environment and diverse teams' representative of the patients and communities we serve.

**Join our Novartis Network**: If this role is not suitable to your experience or career goals but you wish to stay connected to hear more about Novartis and our career opportunities, join the Novartis Network here:
https://talentnetwork.novartis.com/network

**Why Novartis:** Helping people with disease and their families takes more than innovative science. It takes a community of smart, passionate people like you. Collaborating, supporting and inspiring each other. Combining to achieve breakthroughs that change patients' lives. Ready to create a brighter future together?
https://www.novartis.com/about/strategy/people-and-culture

**Benefits and Rewards:** Learn about all the ways we'll help you thrive personally and professionally.
Read our handbook (PDF 30 MB)

Дивизион
Operations
Business Unit
Information Technology
Место
Индия
Сайт
Hyderabad (Office)
Company / Legal Entity
IN10 (FCRS = IN010) Novartis Healthcare Private Limited
Functional Area
Информационные технологии
Job Type
Full time
Employment Type
Regular
Shift Work
No

## Accessibility and accommodation

Novartis is committed to working with and providing reasonable accommodation to individuals with disabilities. If, because of a medical condition or disability, you need a reasonable accommodation for any part of the recruitment process, or in order to perform the essential functions of a position, please send an e-mail to diversityandincl.india@novartis.com and let us know the nature of your request and your contact information. Please include the job requisition number in your message.

Job ID
REQ-10090302

### Assoc. Dir. DDIT ISC Identity & Access Management AD

Apply to Job

Job ID
REQ-10090302

### Assoc. Dir. DDIT ISC Identity & Access Management AD

Apply to Job

---

**Source URL:** *https://www.novartis.ru/careers/career-search/job/details/req-10090302-assoc-dir-ddit-isc-identity-access-management-ad*

**List of links present in page**

1. https://www.novartis.com/careers/benefits-rewards
2. https://talentnetwork.novartis.com/network
3. https://www.novartis.com/about/strategy/people-and-culture
4. https://www.novartis.com/sites/novartis_com/files/novartis-life-handbook.pdf
5. mailto:diversityandincl.india@novartis.com
6. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Assoc-Dir-DDIT-ISC-Identity---Access-Management-AD_REQ-10090302-1
7. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Assoc-Dir-DDIT-ISC-Identity---Access-Management-AD_REQ-10090302-1