ManageEngine
ADManager Plus

Risk exposure management use cases

ManageEngine ADManager Plus

What is risk exposure management in ADManager Plus?

Risk exposure management in ADManager Plus provides a visual representation of potential attack paths that could lead to high-privilege entities—such as Domain Admins or other critical Active Directory groups. It helps IT and security teams identify vulnerable privileged groups, understand how they could be compromised, and take proactive steps to mitigate privilege escalation risks.

The feature maps access paths to privileged groups and monitors them over time. This gives you continuous visibility into how misconfigurations, permissions, or group memberships could be exploited in your Active Directory environment.

The following are a few use cases that will demonstrate the risk exposure management feature:

- Identify users who can escalate to administrator privileges.
- Discover users with DSync privileges.

USE CASE 1

Identify users who can escalate to administrator privileges

Challenge:

Organizations often lack visibility into indirect privilege escalation paths—such as users who aren't Domain Admins but could become one through nested group memberships, misconfigured ACLs, or delegation settings.

How risk exposure management helps:

- Visualizes all potential attack paths leading to privileged groups.
- Helps you uncover users who can attain administrative access through multiple intermediate relationships.
- Provides actionable insights to break or harden risky paths.

Steps to view potential attack paths:

1. Log in to ADManager Plus.
2. Navigate to **Governance > Risk Exposure Management.**
3. Go to the **Privilege Queries Library** and select **Find all Domain Admins.**
4. You can now see a comprehensive list of all users and groups that are members of the Domain Admins group. *[Fig. 1]*

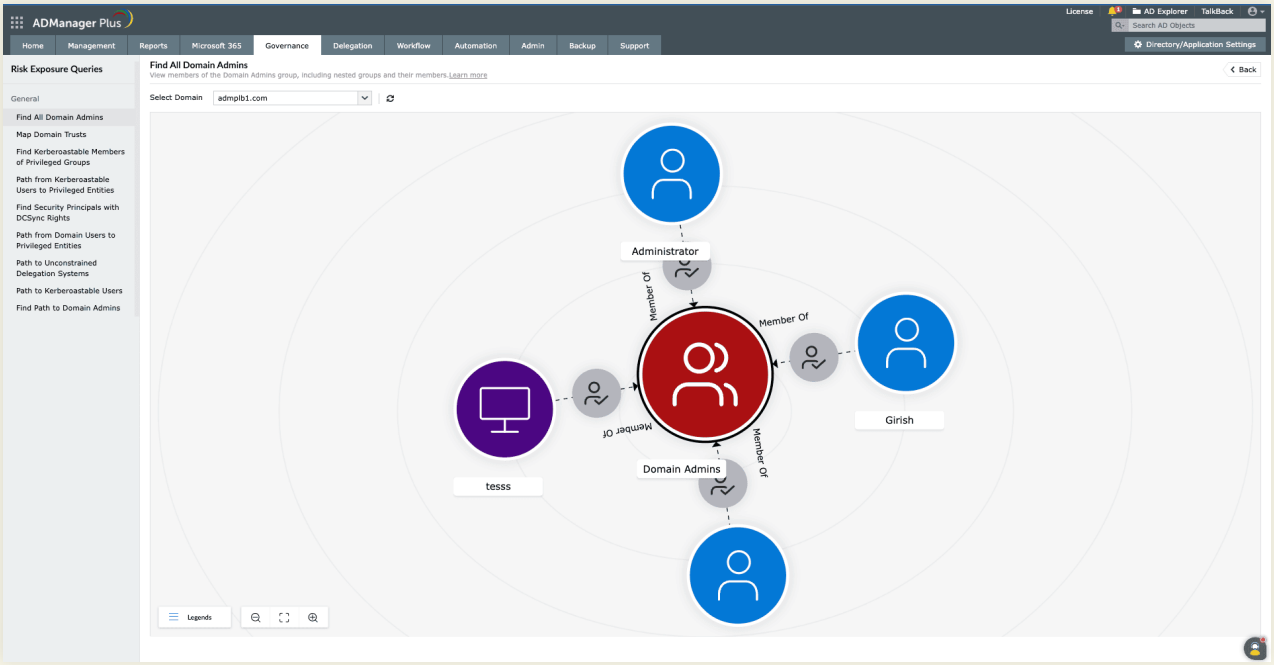

Figure 1. Risk exposure queries in ADManager Plus.

5. Additionally, from the **Privileged Entities Exposure** tab, you can visualize the potential attack flow a malicious actor could exploit to compromise your Domain Admins group.
6. Navigate to **Privileged Entities Exposure.**
7. Locate *Domain Admins* in the *Name* column.
8. Click **View** under the *Attack Flow column. [Fig. 2]*
9. Now, you can view all the possible attack paths that could be exploited to gain control over a privileged entity (here, the Domain Admins group). *[Fig. 3]*
10. Reviewing these flows helps you understand potential risks and proactively strengthen your security posture.

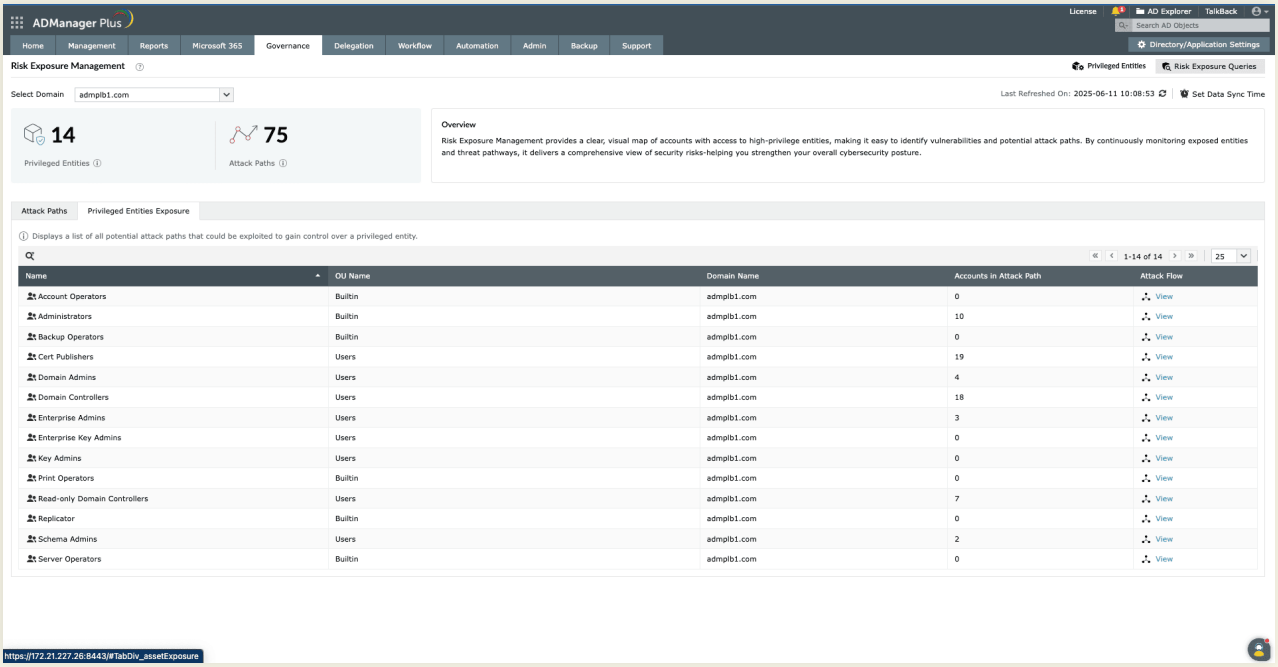

Figure 2. A table displaying Active Directory privileged groups with their attack path visualization links.

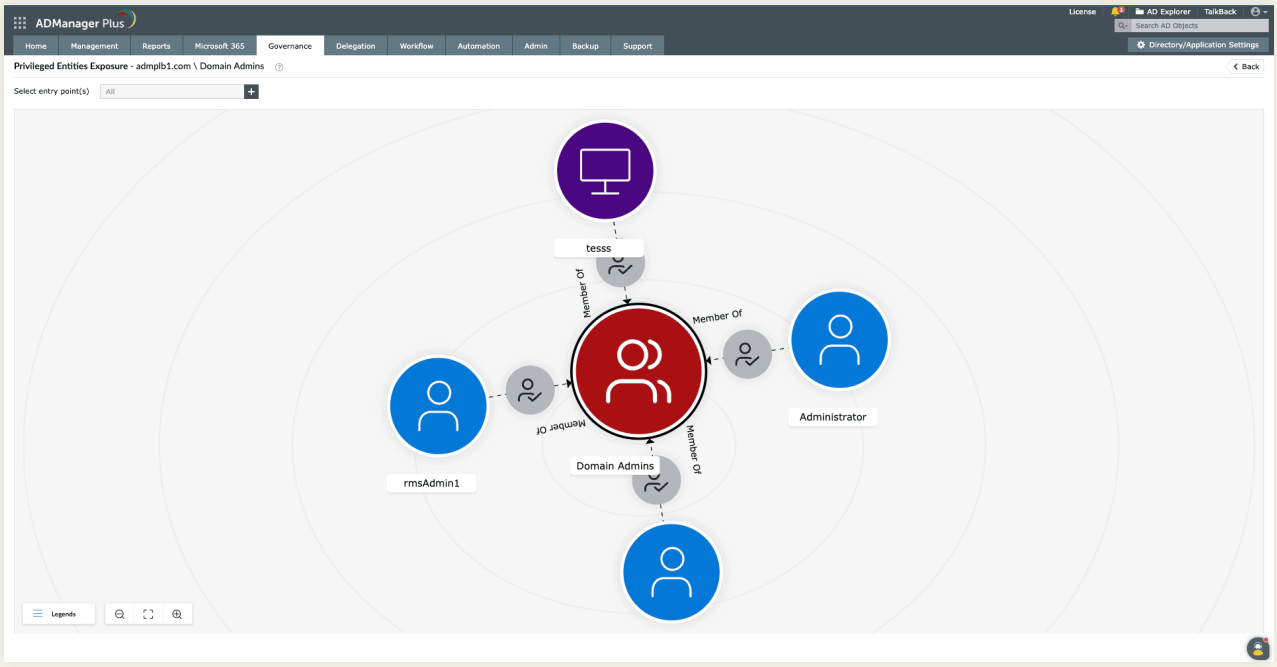

Figure 3. Network diagram showing attack paths to Domain Admins through connected user and group nodes.

Outcome:

Gain clarity on who could gain elevated access—and take action before it's exploited.

USE CASE 2

Discover users with DCSync privileges

Challenge:

Attackers with DCSync rights can replicate sensitive directory data, including password hashes—often without detection. These permissions are hard to track manually.

How risk exposure management helps:

- Includes a privileged queries library to detect accounts and groups with DCSync capabilities.
- Surfaces risky principals with replication permissions on domain controllers.
- Makes it easy to investigate permissions assigned to accounts and how they can be exploited to attack high-risk targets.

Steps to find users and groups with DCSync capabilities:

1. Log into ADManager Plus.
2. Navigate to **Governance > Risk Exposure Management.**
3. Go to the **Privilege Queries Library** and select **Find Principals with DCSync Rights.**
4. This graph visually maps users and groups with DCSync permissions. It helps you view how an attacker could gain full control over your domain by compromising these users and groups. *[Fig. 4]*

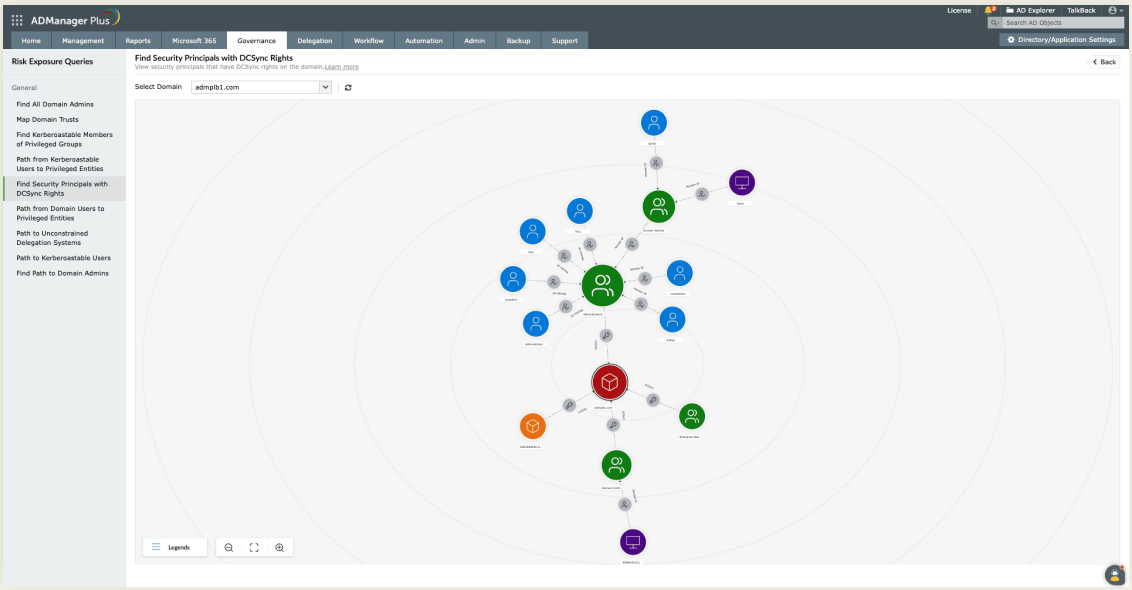

Figure 4. Risk Exposure Queries interface showing prebuilt queries to help identify common security gaps.

Outcome:

Detect and remediate DCSync privileges that could lead to stealthy domain-wide compromise.

ManageEngine
ADManager Plus

Our Products

AD360 | Log360 | ADAudit Plus | ADSelfService Plus

M365 Manager Plus | RecoveryManager Plus

About ADManager Plus

ADManager Plus is an identity governance and administration (IGA) solution that simplifies identity management, ensures security and improves compliance. With ADManager Plus, manage the user life cycle from provisioning to deprovisioning, run access certification campaigns, orchestrate identity management across enterprise applications and protect data on your enterprise platforms with regular backups. Use over 200 reports to gain valuable insights into identities and their access rights. Improve the efficiency of your IGA operations with workflows, automations and role-based access control policies. ADManager Plus' Android and iOS applications help with on-the-go AD and Entra ID management.

For more information about ADManager Plus, visit manageengine.com/products/ad-manager/.

$ Get Quote Download