

Risk exposure management

Visualize, assess, and mitigate privilege escalation
risks in Active Directory



Limited visibility into privileged entities increases security risks



- ◆ Difficult to identify vulnerable privileged groups and access paths
- ◆ Manual investigations are time-consuming and error-prone
- ◆ Attackers exploit privilege escalation paths to gain control
- ◆ Need for continuous monitoring and proactive risk mitigation

What is the risk exposure management in ADManager Plus?



A visual representation of privileged entity risk exposure in AD environments



Maps potential attack paths that can compromise both built-in and custom privileged groups



Identifies vulnerable groups and associated threat pathways



Delivers a complete assessment of privilege escalation vulnerabilities



Displays actionable remediation measures to strengthen your organization's security framework

Risk exposure management dashboard

This indicates the identified potential routes an attacker could take to compromise high-value assets within Active Directory.

1

This highlights all the highly sensitive accounts or groups that, if compromised, could grant an attacker significant control over Active Directory.

2

This column provides a detailed breakdown of the specific relationships and permissions constituting each attack path, visible by clicking "View."

3

ADManager Plus

Home Management Reports Microsoft 365 Governance Delegation Workflow Automation Admin Backup Support

Risk Exposure Management

Select Domain: admplb1.com

Last Refreshed On: 20...

Privileged Entities 14

Attack Paths 75

Overview

Risk Exposure Management provides a clear, visual map of accounts with access to high-privilege entities, making it easy to identify vulnerabilities and potential attack paths. and threat pathways, it delivers a comprehensive view of security risks-helping you strengthen your overall cybersecurity posture.

Attack Paths Privileged Entities Exposure

Displays potential attack paths from an initial point to a privileged entity

Entry point	Parent	Target	Relation	Attack Flow
Administrator	Enterprise Admins	Enterprise Admins	Member Of	View
Administrator	Domain Admins	Domain Controllers	Member Of	View
Administrator	Administrators	Administrators	Member Of	View
Administrator	Domain Admins	Administrators	Member Of	View
Administrator	Enterprise Admins	Cert Publishers	Member Of	View
Administrator	Administrators	Cert Publishers	Member Of	View
Administrator	Enterprise Admins	Domain Controllers	Member Of	View
Administrator	Schema Admins	Schema Admins	Member Of	View
Administrator	Domain Admins	Cert Publishers	Member Of	View
Administrator	Administrators	Domain Controllers	Member Of	View
Administrator	Domain Admins	Domain Admins	Member Of	View
Administrators	ADMPB-DC1	Cert Publishers	Generic Write, Write Owner, Write DACL, All Extend Rights	View
Administrators	ADMPB-DC1	Domain Controllers	Generic Write, Write Owner, Write DACL, All Extend Rights	View
ADMPB-DC1	Domain Controllers	Domain Controllers	Member Of	View
ADMPB-DC1	Cert Publishers	Cert Publishers	Member Of	View
ADMPB-MEM1	Cert Publishers	Cert Publishers	Member Of	View



Visual attack path mapping

Graphical representation of paths attackers might use to gain access to privileged groups. This shows how attackers might reach privileged targets



Privileged group exposure

Identifies built-in and custom groups at risk by mapping potential attack pathways. This shows which privileged targets are exposed and how they are vulnerable



Scheduled data update

Keeps the data up to date for proactive management



Privilege queries library

Pre-built queries for detailed risk insights

What is the risk exposure management in ADManager Plus?



Map attack paths

Visually identify potential routes an attacker could take from entry points to compromise high-value assets within Active Directory.



Identify privileged targets

Highlight all highly sensitive groups that, if compromised, could grant an attacker significant control over Active Directory.



Analyze relationships and permissions

View a detailed breakdown of the specific relationships and permissions that constitute each attack path.

Visualizing Active Directory attack paths

This icon represents the initial point of access or compromise an attacker could leverage, such as a user account.

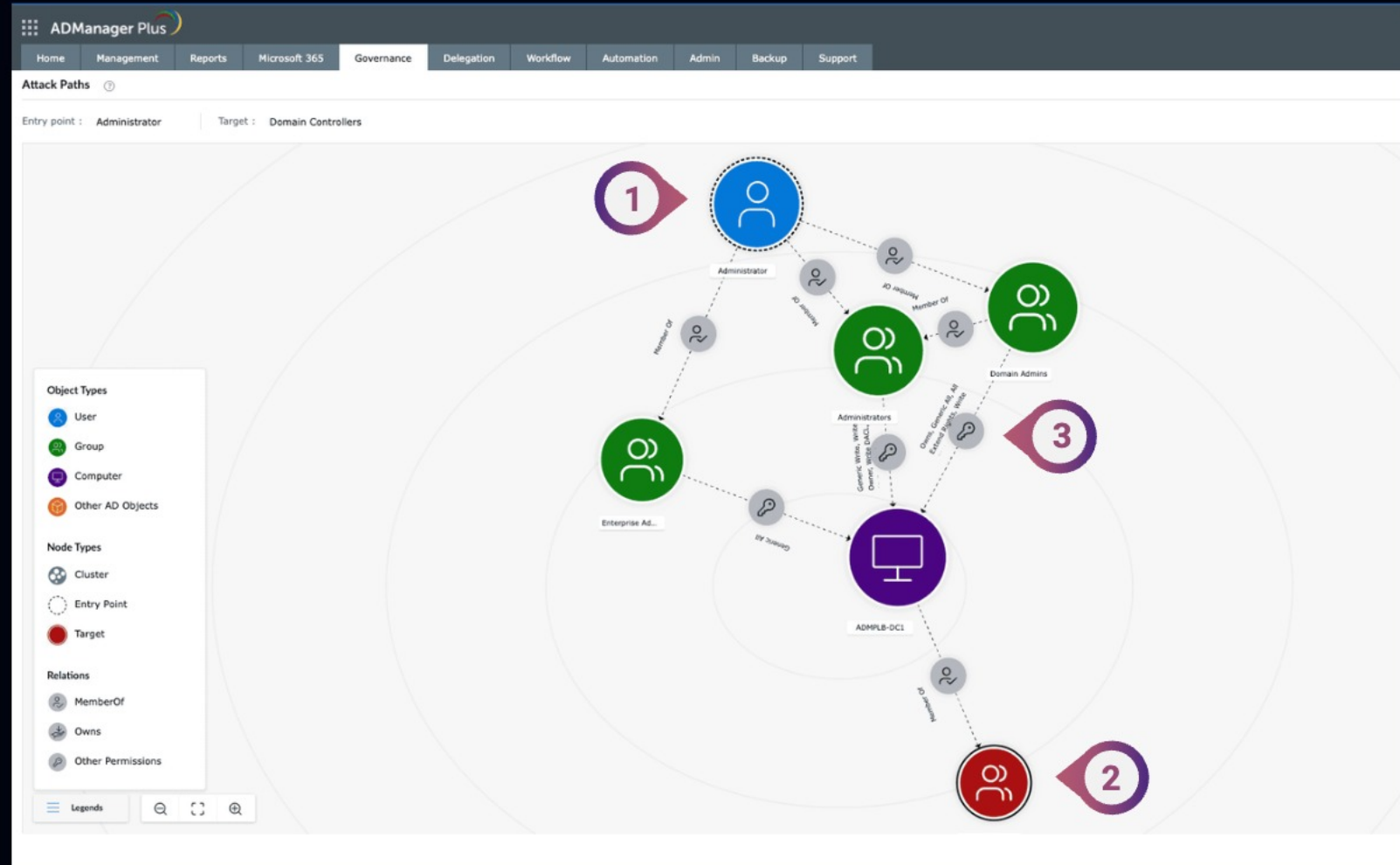
1

This icon signifies the high-value asset or system an attacker aims to reach or control, in this case, "Domain Controllers."

2

The arrows and accompanying text (e.g., "Member Of," "Administrators," "GenericAll") depict the specific relationships and permissions that enable the attack path, illustrating privilege escalation or lateral movement.

3



Privileged group exposure



Identifying privileged groups

- ✓ Lists critical privileged groups (e.g., Domain Admins, Enterprise Admins, Schema Admins)
- ✓ Details their OU and domain names for precise location



Mapping attack paths to privileged access

- ✓ Shows all accounts and assets that form a path leading to these high-value groups
- ✓ Clearly identifies the initial point of compromise or the most vulnerable entry point in each attack path



Visualizing risk—the attack flow

- ✓ Lists critical privileged groups (e.g., Domain Admins, Enterprise Admins, Schema Admins)
- ✓ Details their OU and domain names for precise location

Entry point analysis with access graph

Comprehensive entry point assessment



- ✓ View all privileged entities that can be exploited from a single entry point
- ✓ Navigate through AD Explorer to analyze specific users as potential attack starting points
- ✓ Access detailed entitlements and privilege escalation paths from any selected user
- ✓ Interactive exploration of attack pathways from entry point to privileged targets
- ✓ Click-through analysis of intermediary objects and their role in attack chains
- ✓ Detailed relationship mapping showing how permissions connect entry points to privileged access
- ✓ Built-in remediation guidance for each identified vulnerability path

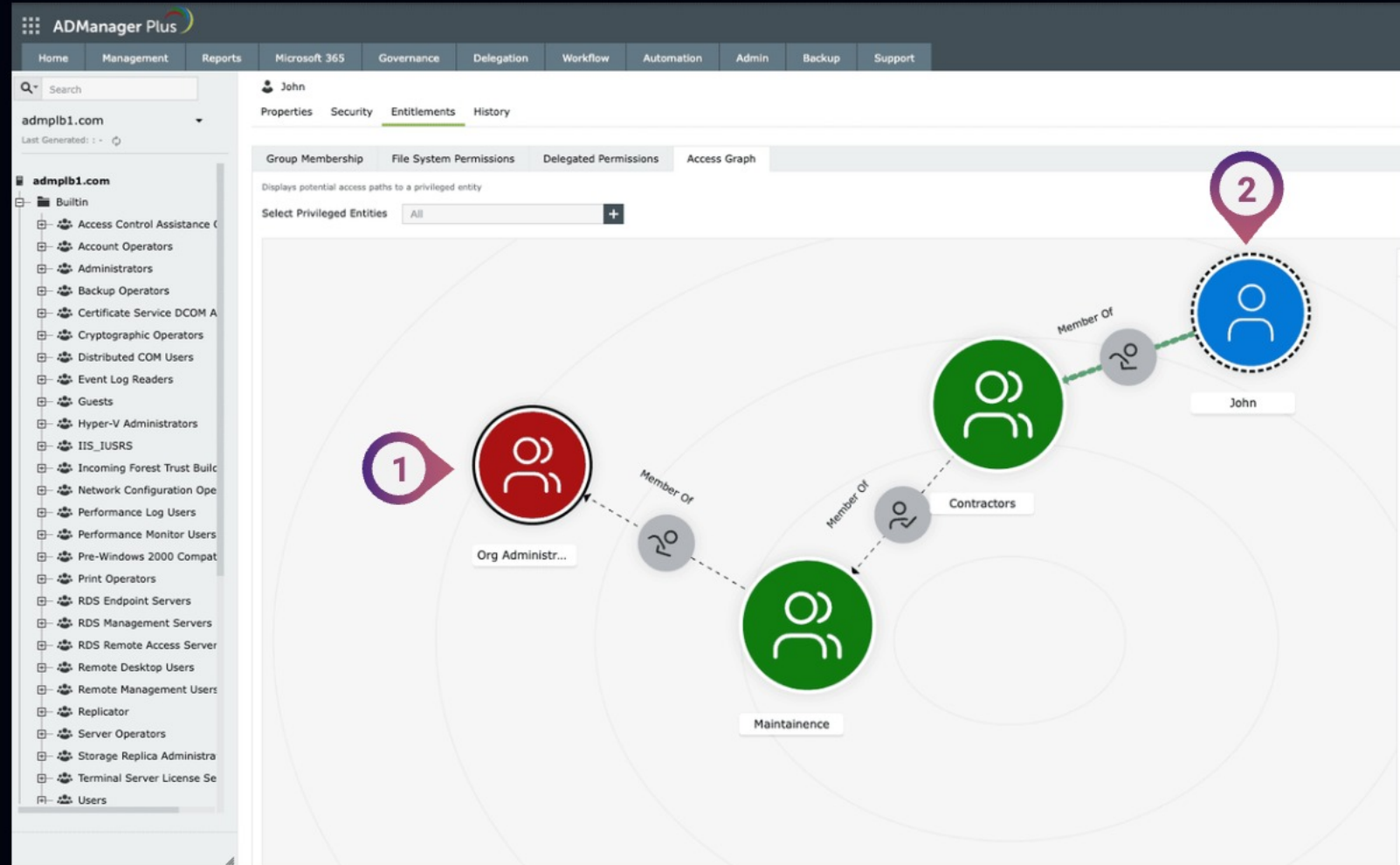
Visualizing Active Directory attack paths

Visually highlights a highly privileged or sensitive Active Directory group, indicating a critical potential target for attackers.

1

The selected identity (user, group, or computer) for whom the access path and potential risk exposure are being analyzed.

2



Relations, permissions, and remediation measures



Access relationship mapping

Visualize complex, permissions-based connections between Active Directory entities that can be leveraged for privilege escalation or lateral movement.



Identify critical exposure

Analyze how seemingly minor permissions contribute to significant security risks and critical exposure paths.



Uncover attack paths

Select any user or group node to investigate their permissions, scope, and role in potential attack chains.



Actionable remediation

Get specific recommendations to reduce exposure by modifying or removing excessive permissions, enabling prioritized remediation based on risk impact.

Risk exposure queries

Provides a library of expert-designed, pre-built queries for rapid identification of common security vulnerabilities



- ✓ Find all members of the Domain Admins group
- ✓ Map domain trust relationships
- ✓ Identify Kerberoastable members of high-value groups
- ✓ Locate principals with DCSync rights
- ✓ Trace paths from domain users to high-value targets
- ✓ And more

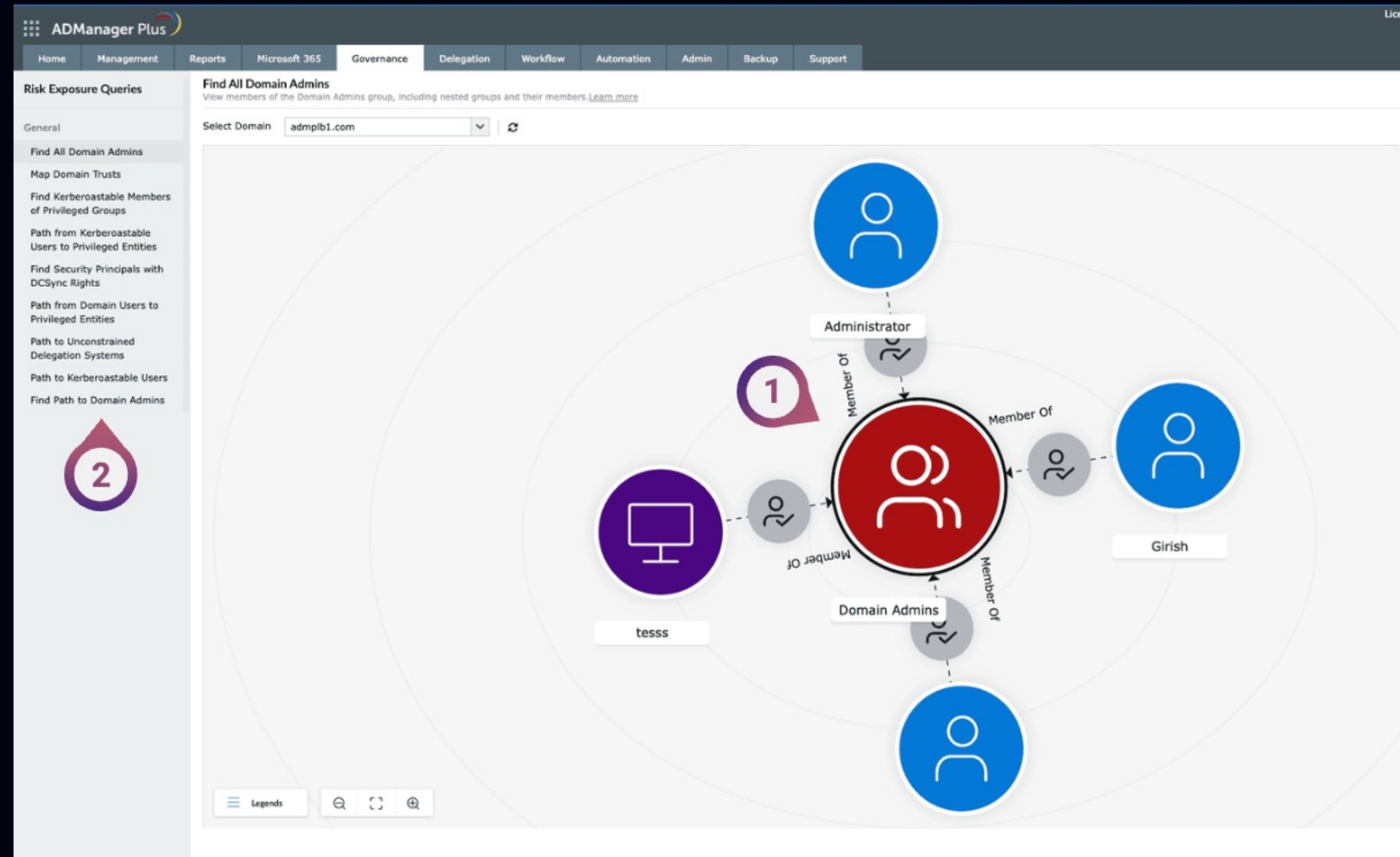
Risk exposure queries library

This central red node highlights the highly privileged 'Domain Admins' group, a critical target for attackers, and shows its members at a glance.

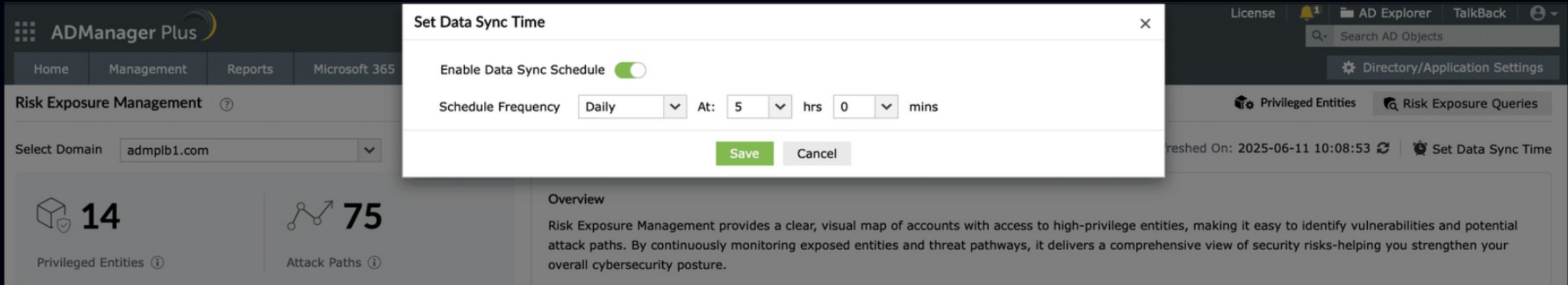
1

The Risk Exposure Queries panel provides pre-built reports to instantly identify specific high-risk configurations and vulnerabilities, such as unconstrained delegations or hidden admin accounts."

2



Continuous monitoring and reporting



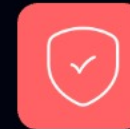
The screenshot displays the ADManager Plus interface. A modal dialog titled "Set Data Sync Time" is open in the center. The dialog includes a toggle switch for "Enable Data Sync Schedule" which is currently turned on. Below this, the "Schedule Frequency" is set to "Daily", and the time is set to "At: 5 hrs 0 mins". "Save" and "Cancel" buttons are at the bottom of the dialog. The background interface shows the "Risk Exposure Management" section with a "Select Domain" dropdown set to "admplb1.com". It displays two metrics: "14 Privileged Entities" and "75 Attack Paths". An "Overview" section provides a summary of the risk exposure management features.



Schedule periodic update of the data

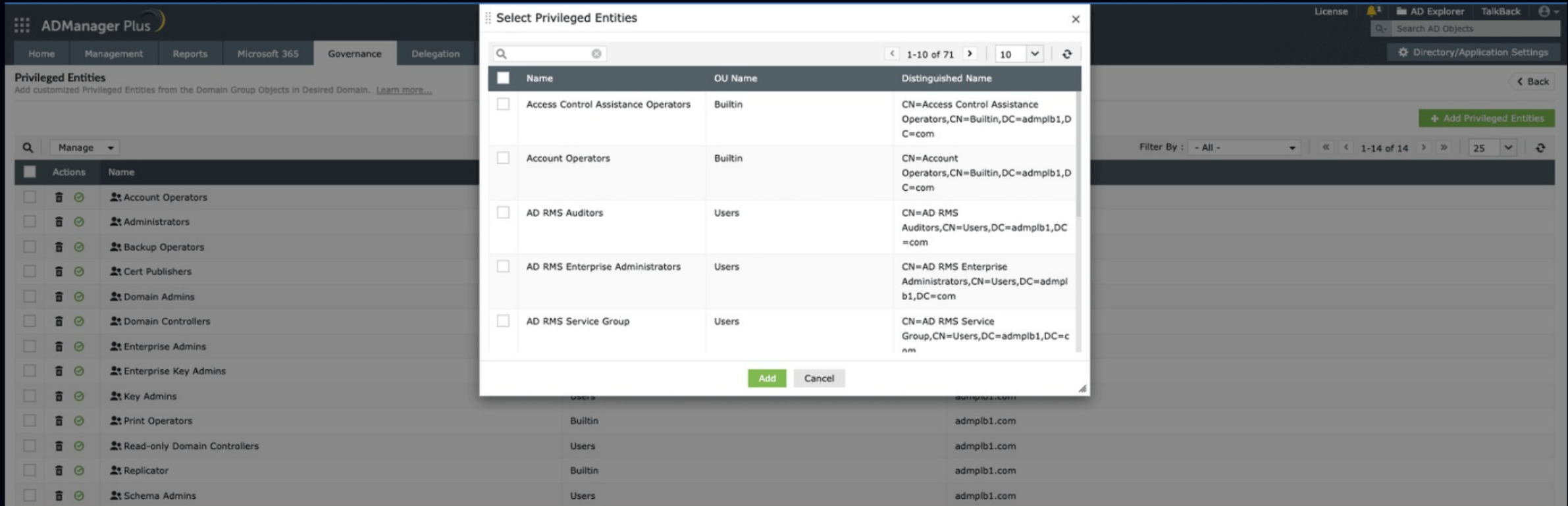


Real-time updates on privileged group exposures and attack paths



Enable security teams to prioritize vulnerabilities and take timely action

Managing privileged Active Directory entities



Privileged Entities
 Add customized Privileged Entities from the Domain Group Objects in Desired Domain. [Learn more...](#)

Search: Manage

Actions	Name
<input type="checkbox"/>	Account Operators
<input type="checkbox"/>	Administrators
<input type="checkbox"/>	Backup Operators
<input type="checkbox"/>	Cert Publishers
<input type="checkbox"/>	Domain Admins
<input type="checkbox"/>	Domain Controllers
<input type="checkbox"/>	Enterprise Admins
<input type="checkbox"/>	Enterprise Key Admins
<input type="checkbox"/>	Key Admins
<input type="checkbox"/>	Print Operators
<input type="checkbox"/>	Read-only Domain Controllers
<input type="checkbox"/>	Replicator
<input type="checkbox"/>	Schema Admins

Select Privileged Entities

Search: 1-10 of 71 10

Name	OU Name	Distinguished Name
<input type="checkbox"/> Access Control Assistance Operators	Builtin	CN=Access Control Assistance Operators,CN=Builtin,DC=admplb1,DC=com
<input type="checkbox"/> Account Operators	Builtin	CN=Account Operators,CN=Builtin,DC=admplb1,DC=com
<input type="checkbox"/> AD RMS Auditors	Users	CN=AD RMS Auditors,CN=Users,DC=admplb1,DC=com
<input type="checkbox"/> AD RMS Enterprise Administrators	Users	CN=AD RMS Enterprise Administrators,CN=Users,DC=admplb1,DC=com
<input type="checkbox"/> AD RMS Service Group	Users	CN=AD RMS Service Group,CN=Users,DC=admplb1,DC=com

This showcases ADManager Plus's *Privileged Entities* management feature, demonstrating how to view existing privileged accounts and the process of adding new ones to monitor and manage their security within the domain.

What you gain with risk exposure management



Proactively uncover and reduce privilege escalation risks



Improve AD security posture with visual, easy-to-understand data



Identify security risks and take immediate action to reduce them



Keep an eye on high-value groups in your AD



Add custom groups to the list of built-in privileged AD groups and monitor access paths to them for potential attacks



Explore risk exposure management

[Start proactively protecting your AD today!](#)