

# Enterprise Reporter Suite

简化了Microsoft平台安全性、合规性和报告

当今的系统和安全管理员负责广泛的任务，包括安全评估、迁移前后分析以及资源优化和分配。他们每天都需要回答类似如下的问题：

- 谁可以在Active Directory (AD)和Azure AD中执行什么操作？
- 哪些邮箱已迁移并驻留在混合Exchange部署中？
- 谁有权访问哪些打印机、共享、文件夹、文件和Microsoft SQL Server数据库？
- 在Azure中托管了什么资源，谁可以访问这些资源？
- 我们的服务器是如何配置的？
- 每台服务器上存在哪些本地用户和组，成员关系是什么？

通过手动方法回答这些问题是一项艰巨的任务，会占用大量时间，将这些时间用在

其他项目上会更好。此外，该任务容易出错，使您容易出现安全违规情况。

仅用一个解决方案便可识别Microsoft系统的当前和历史配置，从而帮助管理员快速高效地回答这些问题。Quest® Enterprise Reporter Suite可助您确保内部部署和基于云的Microsoft环境的安全性及合规性。全面访问评估和内置报告功能有助于深入了解Active Directory/Azure AD、Azure资源、Exchange/Exchange Online、Microsoft Teams、OneDrive for Business、Windows Server、SQL Server、网络连接存储(NAS)和存储区域网络(SAN)，包括用户、组、权限、应用程序、资源、虚拟机(VM)和其他配置。

此外，Enterprise Reporter Suite还包含Quest® Security Explorer®，因此您可以在Enterprise Reporter用户界面中快速执行操作，以删除任何不当权限。

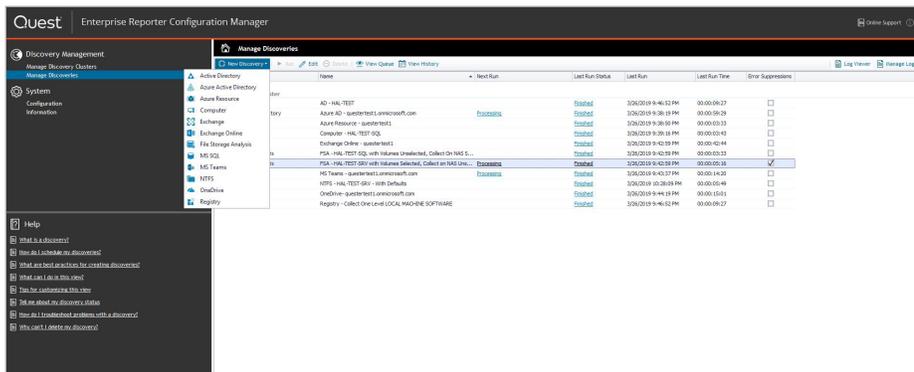


图1: Enterprise Reporter收集、存储和报告Active Directory/Azure AD、Exchange/Exchange Online、Microsoft Teams、OneDrive for Business、Windows Server、SQL Servers、NAS和SAN的配置。

“Enterprise Reporter非常易于使用。报告模板非常有用，而且只需几分钟便可完成自定义以收集所需的数据。”

小型商业银行公司的系统管理员  
来源: TechValidate。

## 优势:

- 针对谁有权访问您的Microsoft环境（包括内部部署和云环境）中的哪些资源，提供实时评估
- 通关直观了解正在创建的Microsoft Teams群组以及它们的使用方式，避免Office 365环境中的组无序增长。
- 通过增加对重要IT资产的可见性并保持职责的适当分离，提高安全性与合规性
- 通过直观地了解租户、订阅和许可服务套餐，来优化Office 365许可证分配和服务套餐决策，并且通过直观地查看虚拟机和磁盘利用率来优化Azure资源。
- 可扩展、安全且可自定义，从而支持具有多个报告使用者组的大型复杂Windows环境

Enterprise Reporter通过对Active Directory/Azure AD、Exchange/Exchange Online、Microsoft Teams、OneDrive for Business、Windows Server、SQL Servers、NAS和SAN的配置进行统一报告，简化Microsoft平台安全性与合规性。

### 系统要求

有关系统要求的完整列表，请查看发行说明。

Security Explorer还提供一系列其他安全功能，如能够从一个中心位置快速授予、撤销、克隆、修改和覆盖权限。此报告和修正功能组合可以提高安全性与合规性，帮助提前防范安全漏洞，避免数据泄露。

### 特性

#### Enterprise Reporter特性

- **直观显示安全性与合规性** - 通过采取安全妥善做法，明确内部策略和外部法规并了解您的Windows环境中所有重要IT资产的配置，从而增强合规性。
  - **Active Directory/Azure AD** - AD用户、组、角色、组织单位和权限；Azure AD用户、组、角色和应用程序服务主体
  - **Exchange/Exchange Online** - 邮箱、邮箱文件夹、启用邮件的用户、通讯组、公共文件夹、权限等
  - **Office 365** - Azure AD、Exchange Online、Microsoft Teams和OneDrive for Business中重要IT资产的配置
  - **Windows Server** - 内部部署共享、文件、文件夹、打印机、注册表项和服务
  - **OneDrive for Business** - 文件和文件夹权限，包括是否可以在内部或外部共享内容
  - **SQL Server** - 数据库安全配置，包括用户、登录、角色和数据库权限
  - **Azure资源** - 虚拟机、磁盘、网络安全组、存储帐户等
- **访问评估** - 了解谁有权访问企业网络中的哪些资源。严格按需提供访问权限，以增强安全性并通过IT审核。
- **直观了解租户、订阅和许可** - 通过直观了解租户、订阅和许可服务套餐，轻松优化Office 365许可证分配和服务套餐决策。
- **托管资源优化** - 通过深入了解虚拟机和磁盘部署（包括配置的数量、规模和方式等）来优化Azure资源使用，以便节省不必要和未充分利用的资源。
- **迁移前后分析** - 通过更加深入地了解用户和组依赖项、对象匹配和潜在冲突、未使用或禁用的帐户以及资源、计算机文件及文件夹所在的位置，为迁移或整合项目做好规划。在开始迁移之前轻松确定需要迁移的内容，并在迁移后确保已迁移正确的数据和权限。
- **Microsoft Teams评估** - 快速发现和报告Office 365环境中存在的Microsoft Teams群组、这些群组的成员以及群组的使用方式。通过Enterprise Reporter for Office 365可以轻松控制Microsoft Teams群组增长，从而避免组无序增长并监控使用情况。
- **借助Quest IT安全搜索提高洞察力** - 将大量系统和设备中的不同IT数据关联到交互搜索引擎，以加快安全事件响应和取证分析速度。通过丰富的可视化和事件时间表囊括用户授权和活动、事件趋势、可疑模式等。
- **容量规划** - 报告和管理各种设备上的存储容量规划和分配，包括Windows文件服务器、NAS和SAN。
- **可扩展的数据收集** - 扩展到位于不同地理位置的任何规模的环境。将收集工作安排在非高峰时段，以尽量降低数据收集对网络和服务器性能的影响，并利用分布式收集体系结构实现负载均衡。
- **高效的存储** - 通过比较发现的内容并只存储更改的内容，减少数据库存储需求并保存更多更改历史数据。
- **自动化报告 workflow** - 通过自动化报告生成功能和灵活的报告交付计划，确保利益相关者在需要时获得所需的报告。
- **职责分离(SoD)** - 通过为审计员、帮助台人员、IT经理以及其他利益相关者准确提供所需的报告（没有多余内容），严格遵守部门和业务职能划分。

## 按类别列出的内置报告示例

### Active Directory报告:

有关用户、组、域等方面的信息  
复制域和匹配（计算机、组、用户）

### Azure Active Directory报告:

租户信息  
应用程序服务器主体  
Azure用户、角色、组和成员

### Microsoft Teams:

群组 and 成员  
群组所有者信息

### Azure资源:

资源访问、组、订阅信息  
存储帐户信息  
虚拟机和磁盘信息

### OneDrive for Business报告:

配置设置  
驱动器信息和权限

### Exchange/Exchange Online:

通讯组  
邮箱权限  
公共文件夹权限

### Windows文件服务器:

文件和文件夹信息与权限

### 混合:

OneDrive和  
NTFS文件和文件夹权限

### SQL Server:

实例、权限、角色、用户等

### 文件存储分析:

容量规划  
文件和文件夹、共享和用户报告  
[查看完整报告列表](#)

- **可自定义的报告** - 使用预定义的报告或创建新报告，执行满足贵组织独特信息需求的有效数据分析。使用高级筛选功能进行自定义，并可导出多种格式的报告，包括PDF、HTML、MHT、RTF、XLS、XLSX、CSV、文本和图像。
- **通用报告门户** - 将报告导出到我们的[软件知识门户](#)，以在整个Quest安全与合规性解决方案中实现统一的报告界面。

## Security Explorer特性

- **集中化的权限管理** - 通过授予、撤销或修改权限对服务器执行针对性更改或批量更改。在资源的访问控制列表中直接查看和管理组成员身份设置。通过对受保护的對象强制应用权限，修复“访问被拒绝”错误。
- **企业范围的权限审查** - 无需手动搜索每个服务器来获得权限。搜索AD、文件服务器、Exchange服务器、SQL Server和SharePoint上的继承权限或显式权限。甚至可搜索服务、任务、用户和组的权限。
- **高级安全性和权限** - 快速备份权限，为您的访问控制设定基准。如果发生意外或恶意更改，则可随时轻松恢复到该基准，而无需恢复数据。提高安全性并确保强制实施合规性要求。

- **全面的报告** - 导出数据库或电子表格，列出目录树中任意位置的项目的权限。筛选结果，以仅显示与父文件夹不同的权限。在整个网络中有针对性地搜索特定组或用户可以访问的所有位置，并导出此类数据，以创建临时安全性报告。

- **直观的访问控制** - 将安全设置备份和还原到替代位置，因此您可确保在新服务器上应用适当的访问权限。

## 关于QUEST

Quest致力于为瞬息万变的企业IT领域提供软件解决方案。我们帮助简化数据爆炸、云扩展、混合数据中心、安全威胁以及合规要求所带来的挑战。我们的产品组合包括用于数据库管理、数据保护、统一端点管理、身份和访问管理以及Microsoft平台管理的解决方案。