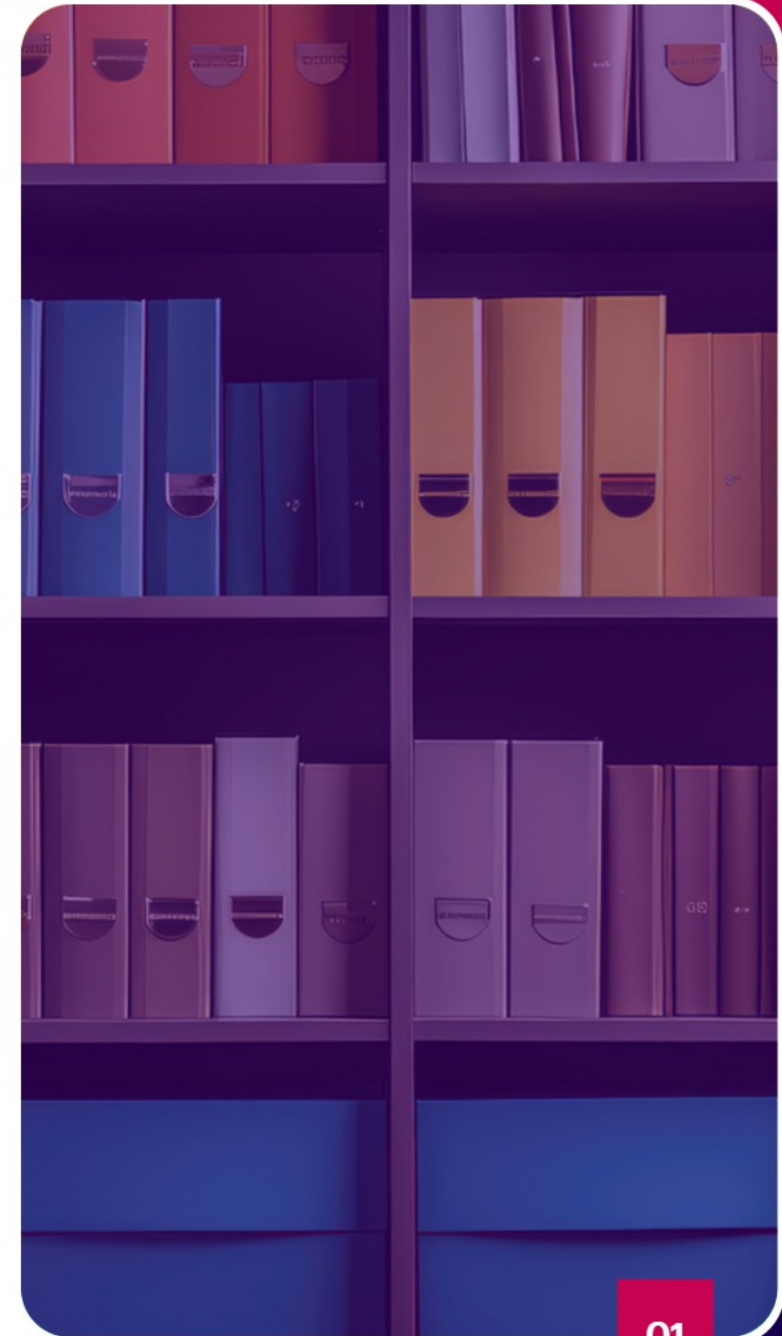


**Improve productivity,  
assess identity threats,  
and achieve compliance**  
with ADManager Plus' reports

# What's inside?

- ✓ ADManager Plus' report library
- ✓ The custom report builder
- ✓ How to run custom reports
- ✓ Risk assessment reports
- ✓ How does it work?
- ✓ Compliance and ADManager Plus
- ✓ How ADManager Plus' reports helped Essentia Health
- ✓ Additional capabilities



# ADManager Plus' report library

- ✓ Access over 150 built-in reports with different categories covering AD, Microsoft 365, and Google Workspace
- ✓ Manage objects right from within the reports
- ✓ Avoid missing out on critical insights by scheduling reports to run automatically at specified time intervals



# ADManager Plus' report library

## Active Directory reports on



Users  
Passwords  
NTFS permissions  
And more!

## Microsoft 365 reports on



Users  
Security  
And more!

## Google Workspace reports on



Active users  
Suspended users

Get a glimpse of the different types of reports

The screenshot displays the ADManager Plus interface with the 'Reports' section selected. The top navigation bar includes 'License', 'AD Explorer', 'TalkBack', and a search bar for 'Search AD Objects'. Below the navigation, there are tabs for 'Microsoft 365', 'Delegation', 'Workflow', 'Automation', 'Admin', 'Backup', and 'Support'. A secondary row of tabs lists report categories: 'Password Reports', 'Group Reports', 'Computer Reports', 'Exchange Reports', 'GPO Reports', 'NTFS Reports', and 'More'. On the left, a sidebar menu lists report types: 'User Reports', 'Password Reports', 'Group Reports', 'Computer Reports', 'Exchange Reports', 'Contact Reports', 'Terminal Service Reports', 'GPO Reports', 'OU Reports', 'NTFS Reports', 'Security Reports', 'Other Reports', 'Compliance Reports', 'Google Workspace Reports', and 'Custom Reports'. At the bottom of the sidebar is a link for 'Identity Risk Assessment' with a 'NEW' badge. The main content area is titled 'User Reports' and is divided into several sections: 'General Reports' (All Users, Users in more than one group, Lync/Skype Enabled Users, etc.), 'Logon Reports' (Inactive Users, Real Last Logon, etc.), 'Nested Reports' (Users in Groups, Groups for Users), 'Account Status Reports' (Disabled Users, Locked-out Users, etc.), and 'CSV Import' (Report from CSV). A 'Schedule Reports' button is located in the top right of the main content area.

Schedule reports to be sent via email

Schedule Reports

ADManager Plus

License | AD Explorer | TalkBack

Search AD Objects

Home | Management | **Reports** | Microsoft 365 | Delegation | Workflow | Automation | Admin | Backup | Support

User Reports | Password Reports | Group Reports | Computer Reports | Exchange Reports | GPO Reports | NTFS Reports | More

**Password Expired Users**

Selected Domain:  admanagerplus.com  
Selected OUs: All [Add OUs](#)

Generate Stop

Generated on: 2024-01-23 04:05:27

Export as: CSV, PDF, XLSX, HTML, CSVDE

Schedule Reports

Exclude Disabled Users

+ Create Request

|                          | SAM Account Name | Password Last Set     | Password Expiry Date | Object Class        | Password Status | PSO Applied | Account Status |
|--------------------------|------------------|-----------------------|----------------------|---------------------|-----------------|-------------|----------------|
| <input type="checkbox"/> | -                | krbtgt                | 2023-04-28 08:27:56  | 2023-06-09 08:27:56 | user            | Expired     | Disabled       |
| <input type="checkbox"/> | -                | \$631000-D4TU58J96II7 | 2023-11-23 11:53:06  | 2024-01-04 11:53:06 | user            | Expired     | Disabled       |
| <input type="checkbox"/> | -                | CTest                 | 2023-11-30 13:38:51  | 2024-01-11 13:38:51 | user            | Expired     | Enabled        |
| <input type="checkbox"/> | -                | David                 | 2023-12-04 17:28:35  | 2024-01-15 17:28:35 | user            | Expired     | Enabled        |
| <input type="checkbox"/> | -                | ralotaibi             | 2023-12-12 03:56:14  | 2024-01-23 03:56:14 | user            | Active      | Disabled       |
| <input type="checkbox"/> | bala jk          | bala                  | 2023-11-16 08:27:49  | 2023-12-28 08:27:49 | user            | Expired     | Enabled        |
| <input type="checkbox"/> | helpdeskcol      | helpdeskcol           | 2023-11-16 10:52:24  | 2023-12-28 10:52:24 | user            | Expired     | Enabled        |

Export the reports in convenient formats

Implement a business workflow from the report itself

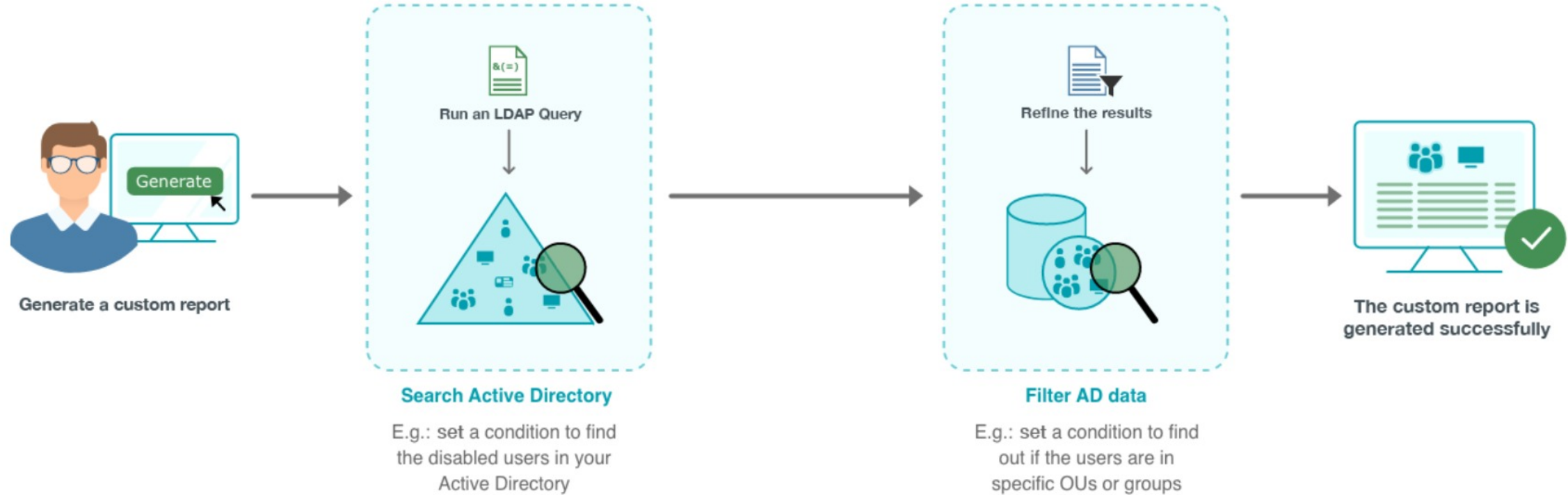
# The custom report builder

- ✓ Build custom reports from scratch with criteria-based LDAP queries and advanced filters for unique scenarios
- ✓ Refine the results of a report with specific conditions to get a curated list of the objects you want

The screenshot shows the 'Custom Report' configuration page in ADManager Plus. The interface includes a navigation menu with options like Home, Management, Reports, Microsoft 365, Delegation, Workflow, Automation, Admin, Backup, and Support. The 'Reports' section is active, showing a dropdown menu with categories like User Reports, Password Reports, Group Reports, Computer Reports, Exchange Reports, GPO Reports, and NTFS Reports. The main configuration area is titled 'Custom Report' and contains the following fields:

- Report name:** 'Recently created but never logged on us'
- Description:** 'View all user accounts that were created in the last 30 days but never logged on.'
- Add report to:** 'User Reports'
- Select domains:** A list of domains with checkboxes and 'Add OUs' links:
  - xcross.com Selected OUs: All Add OUs
  - child.xcross.com Selected OUs: All Add OUs
  - csez.zohocorpin.com Selected OUs: All Add OUs
  - ycross.com Selected OUs: All Add OUs
- Conditions:** A section for defining filters, currently showing:
  - Users +
  - Filters Columns Management Actions
  - LDAP Filter
  - 1. When Created Last 30 days
  - Criteria : (1)

# How to run custom reports





# Risk assessment reports

- ✓ Understand your AD and Microsoft 365 risk posture through risk scores
- ✓ Access one-click reports on the threat indicators to find out your potential security gaps and fix them

The risk score and the severity of the risks

**Identity Risk Assessment**

**Risk Score**

39 / 100  
Your Risk Score is **Medium**  
[How is the Risk Score calculated?](#)

**Summary**

Our "Identity Risk Assessment" tool aims to empower organizations in their battle against active risks or vulnerabilities in their identity-environment. The tool provides a clear and comprehensive view of potential risks, enabling IT administrators to enhance the overall security and stability of the identity network. Instead of just reacting to security incidents as they occur, our tool enables you to take a proactive stance against identity-based attacks by scanning and assessing your identity-infrastructure, evaluating and prioritizing risks based on severity, generating detailed risk reports, and offering prescriptive risk-remediation guidance. [Learn More...](#)

**User** | Computer | Group | GPO | Filter By: All

| Privileged users                         |          |                | Non-privileged users                     |          |                  |
|------------------------------------------|----------|----------------|------------------------------------------|----------|------------------|
| Risk Name                                | Severity | Risk Exposure  | Risk Name                                | Severity | Risk Exposure    |
| Inactive Users                           | High     | 0% ( 0 of 1)   | Inactive Users                           | Medium   | 100% ( 13 of 13) |
| Disabled Users                           | Low      | 0% ( 0 of 1)   | Disabled Users                           | Low      | 19% ( 3 of 16)   |
| Users with Unchanged Passwords           | High     | 100% ( 1 of 1) | Users with Unchanged Passwords           | Medium   | 38% ( 6 of 16)   |
| Users Never Logged On                    | High     | 0% ( 0 of 1)   | Users Never Logged On                    | Medium   | 81% ( 13 of 16)  |
| Users With Password Not Required Enabled | Critical | 0% ( 0 of 1)   | Users With Password Not Required Enabled | High     | 13% ( 2 of 16)   |
| Users Whose Password never expires       | High     | 100% ( 1 of 1) | Users Whose Password never expires       | Medium   | 13% ( 2 of 16)   |

ADManager Plus

License | AD Explorer | TalkBack | Search AD Objects | Domain/Tenant Settings

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

Identity Risk Assessment

- Privileged users
- Inactive Users
- Disabled Users
- Users with Unchanged Passwords**
- Users Never Logged On
- Users With Password Not Required Enabled
- Users Whose Password never expires
- Members of Privileged Groups
- Non-privileged users
- Inactive Users
- Disabled Users
- Users with Unchanged Passwords
- Users Never Logged On
- Users With Password Not Required Enabled
- Users Whose Password never expires
- Computer
- Disabled Computers
- Inactive Computers
- Computers Trusted with

### Users with Unchanged Passwords

100%

Risky objects - 1 of 1

Severity : High | Weight : 8

Domain : apple.local

Reset Passwords

|                          | Display Name | Common Name   | SAM Account Name |
|--------------------------|--------------|---------------|------------------|
| <input type="checkbox"/> | -            | Administrator | Administrator    |

Learn what to do after identifying risks

#### Users with Unchanged Passwords

**Description**

Privileged users who have not changed their password in the configured time period.

**Likelihood of compromise**

Accounts with unchanged passwords are more prone to insider attacks and can be compromised by password spraying, credential theft, Kerberoasting, and brute force attacks, especially when their passwords are default, common, or weak. Compromised privileged accounts can help attackers gain access to resources and sensitive data.

**Remediation measures**

Enforce a strong password policy, implement MFA, and perform regular audits in your organization.

**Security frameworks**

**MITRE Attack**

- Persistence
- Privilege Escalation
- Credential Access

**ANSSI**

- Privileged account passwords age too old

# How does it work?

## Risk score

ADManager Plus analyzes identity risks in your AD and Microsoft 365 landscapes through three phases of computation

**Phase 1:** Determines the severity of risks

**Step 1:  
Likelihood  
determination**

Calculates the opportunities for possible threat incidents and the degree of harm if the threats materialize

**Step 2:  
Impact analysis**

Analyzes potential consequences of the risk based on the confidentiality, integrity, and availability (CIA) triad  
Potential consequences include damage to business operations, financial loss, and reputational harm

**Step 3:  
Severity level  
assignment**

Categorizes the risk as low, medium, high or critical from the results of **Step 1** and **Step 2**

**Phase 2:**

Gives risk indicators weightage on a scale from 1 to 10 to calculate the risk exposure of each

**Risk indicators  
include:**

- Privileged users
- Non-privileged users
- Computers  
Groups and  
GPOs

**Phase 3:**

Gives the overall risk score based on the values obtained from **Phase 1 and 2**

# Compliance and ADManager Plus

- ✓ Satisfy compliance mandates using reports

We offer compliance reports for



SOX



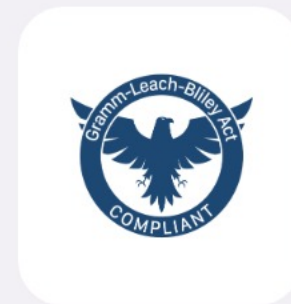
HIPAA



PCI DSS



FISMA



GLBA



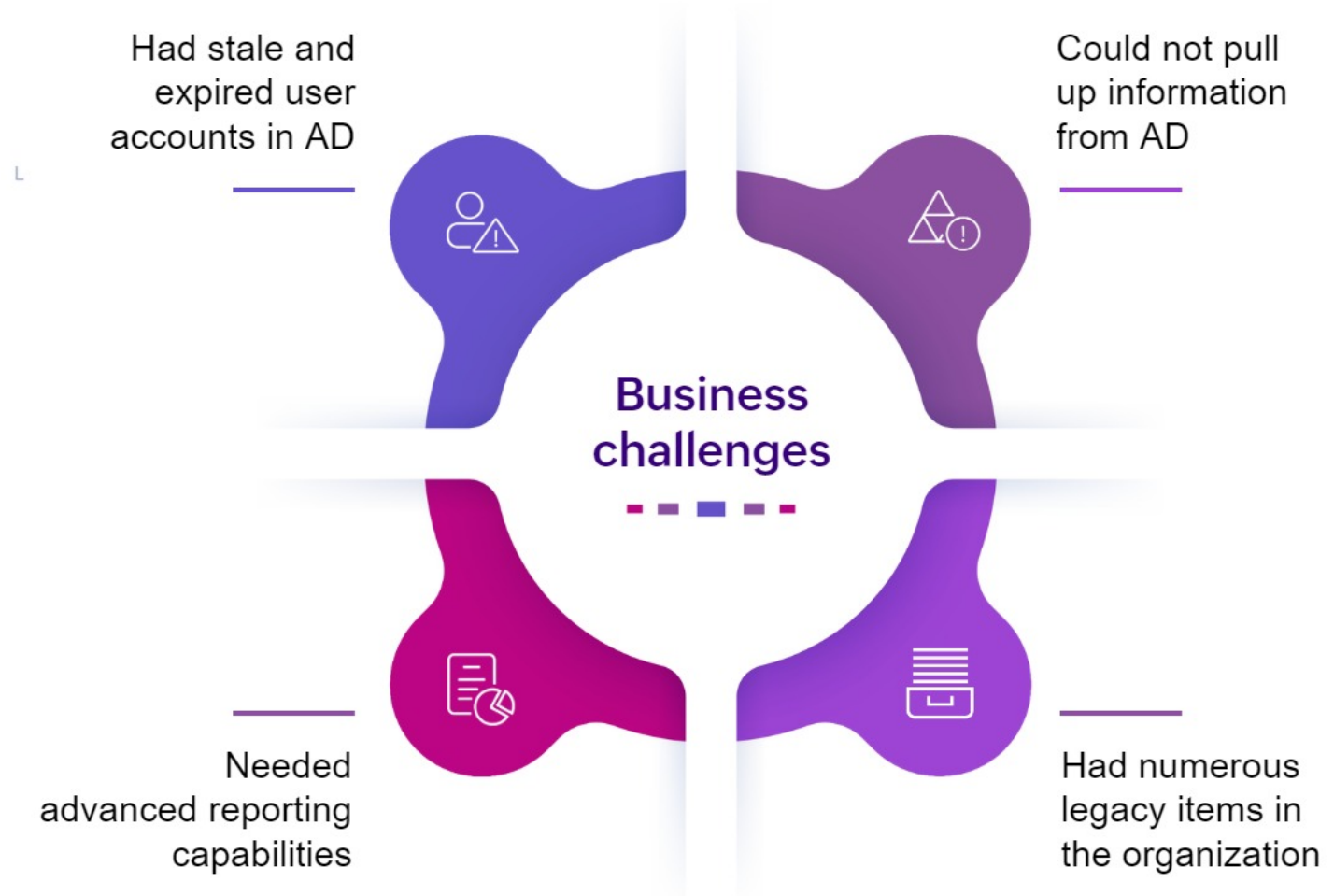
GDPR

# Compliance and ADManager Plus

The screenshot displays the ADManager Plus web interface, specifically the 'Compliance Reports' section. The interface features a top navigation bar with tabs for Home, Management, Reports, Microsoft 365, Delegation, Workflow, Automation, Admin, Backup, and Support. A search bar for AD Objects is located in the top right. The left sidebar contains a navigation menu with categories like User Reports, Password Reports, Group Reports, Computer Reports, Exchange Reports, Contact Reports, Terminal Service Reports, GPO Reports, OU Reports, NTFS Reports, Security Reports, Other Reports, Compliance Reports, Google Workspace Reports, and Custom Reports. The main content area is titled 'Compliance Reports' and is organized into four columns: SOX, HIPAA, PCI, and FISMA. Each column lists various report types, such as 'All Users', 'Recently Logged On Users', 'Recent Logon Failures', 'Real Last Logon', 'Users With Terminal Server Access', 'Recently Created Users', 'Recently Modified Users', 'Recently Modified GPOs', 'Shares in the Servers', 'Permissions for Folders', 'Folders accessible by Accounts', 'Server Permissions', 'Subnet Permissions', 'Servers accessible by Accounts', and 'Subnets accessible by Accounts'. A 'Schedule Reports' button is located in the top right corner of the main content area. At the bottom left of the sidebar, there is a 'Identity Risk Assessment' feature marked as 'NEW'.

# How ADManager Plus' reports helped Essentia Health

ADManager Plus provided fine-grain reports and the option to create custom reports from scratch, which turned out to be such a relief for Essentia Health's IT admins





**Explore more about**  
**[ADManager Plus](#)**  
**right away!**