An Essential Guide to Creating **Custom Reports** Using ADManager Plus

❙ Introduction

Prebuilt reports don't offer admins the option to customize reports to meet their organization's constantly changing requirements. To overcome this challenge, ADManager Plus' Custom Reports feature allow admins to:

- Filter data to narrow their results based on their exact requirements.

- Create reports that include custom attributes in their Active Directory (AD).

- Build reports based on LDAP queries.

- And more.

❙ Filtering report data to meet specific requirements

When generating AD reports, a major concern for many admins is that prebuilt reports contain too much irrelevant information. Even if some reports allow them to customize the fields displayed in the report, it can be difficult to find the information they need. To make reports display only relevant information, admins often have to export reports to a spreadsheet and filter them manually. This process can be made more efficient by using ADManager Plus, which allows admins to set filters and fetch their exact requirements in a report.

Use case: An organization wants to generate a report for members of their marketing team who joined more than a month ago and haven't reset their password in the last 30 days; more specifically, they only want information for marketers working on five different products (A, B, C, D, and E). Since this requirement is very specific, this organization's admins would have to generate a report and then manipulate it in a spreadsheet to get the information they need.

▌ How to filter report data using ADManager Plus

1. Select the **AD Reports** tab.

2. Select **Custom Reports** from the left navigation pane.

3. Click **New custom report**.

4. Specify a **Report Name** and add details about the report under **Description**. For example:

   Report name: Marketing team password reset report

   Description: A report to generate the list of Marketing team members of five different products (A, B, C, D, and E) who joined more than a month ago and have not reset their password in the last 30 days.

5. In the **Add report to** section, select **User Reports**.

6. Choose the appropriate domain from the **Select Domain** list. Select the OUs for these five products (also named A, B, C, D, and E in our example).

7. In the **Conditions** section, select the **Users** object type from the drop-down list.

8. In the **Filters** section, select **Click to Add**. From this list, select:
   When Created attribute -> Before N days -> 30
   AND Password Last Set -> Before N days -> 30
   AND Department Is Marketing

9. In the next section, you can select the details to be displayed in the report, such as **First Name, Last Name, Email Address, Employee ID, Manager**, and so on.

10. Click **Save**.

11. Now that you've created the report, you can export it in PDF, XLS, CSV, or HTML format using the **Export as** option.

Creating reports based on custom AD attributes

Organizations often have to store some information using attributes that are not available in native AD. When the need arises, the Active Directory schema can be extended to include additional attributes that can store this information. For instance, organizations may extend the User class to store additional information such as social security numbers, passport details, gender, birthday, etc., or modify the Computer class to store asset ID, location, and so on.

Unfortunately once an organization extends their AD schema, they won't be able to generate reports based on the value defined in these custom attributes using prebuilt reports. For that kind of reporting, custom attribute-based reports are essential.

Use case: An organization wants to generate a series of reports based on the values of specific schema attributes, including their custom attribute, technicalteamAttribute, that they created to define the specific user account function. They want to create reports that include details such as last logon time, password expiration, and more based on that custom attribute; the report needs to be generated for various values of technicalteamAttribute, such as networking, server, and so on.This makes it easy for the organization to monitor each technical team and share a particular team's report amongst team members.

How to create custom attribute-based reports using ADManager Plus

1. Select the **AD Reports** tab.

2. Select **Custom Reports** from the left navigation pane.

3. Click **New custom report**.

4. Specify a **Report Name** and add details about the report under **Description**. For example:

    Report Name: Technical team report - Networking

    Description: A report to generate the last logon times and password expiration details of the networking team.

5. In the **Add report to** section, select the **User Reports** category.

6. Choose the appropriate domain from the **Select Domain** list.

7. In the **Conditions** section, select the **Users** object type from the drop-down list.

8. In the **Filters** section, select Click to **Add**. From this list, select technicalteamAttribute listed under **Configured Custom Attribute.**

9. In the next section, you can select the details about the users in the networking team which have to appear in the report. Here, select details such as **First Name, Last Name, Email Address, Last Logon Time, Password expires in**, and so on.

5

10. **Click Save.**

11. Now that you've created the report, you can export it in PDF, XLS, CSV, or HTML format using the **Export as** option.

Creating a report based on LDAP queries

If administrators can't meet their reporting requirements using prebuilt reports, they can use LDAP queries to generate the required reports instead. Sometimes technicians may prefer to use the LDAP queries they already have, instead of setting filters available in the custom reports.

Use case: An organization wants to generate a report to find all users whose accounts are enabled but have not logged in for the past 30 days.

How to create LDAP query-based reports using ADManager Plus

1. Select the **AD Reports** tab.

2. Select **Custom Reports** from the left navigation pane.

3. Click **New custom report**.

4. Specify a **Report Name** and add details about the report in **Description**. For example:
   Report name: Account enabled but inactive users
   Description: A report to find all users whose accounts are enabled but have not logged in for the past 30 days.

5. In the **Add report to** section, select the **User Reports** category.

6. Choose the appropriate Domain from the **Select Domain** list.

Custom Report

Report name	Account enabled but inactive users
Description	A report to find users whose accounts are enabled but have not logged in for the past
Add report to	User Reports

▼ **Select domains**

☑ admplab.com   ☐ csez.zohocorpin.com
   Selected OUs : All [Add OUs]

7. In the **Conditions** section, select **Custom query** from the drop-down list.

8. Enter the query below in the space provided:
   (&(objectCategory=person)(objectClass=user)(&(!(userAccountControl:1.2.840.113556
   1.4.803:=2))(lastLogon<=131556638360000000)))

9. Select the necessary details to be displayed for this report, such as **SAM Account Name, Email Address, Employee ID, Department, Manager**, and so on.

10. Click **Save**.

11. Now that you've generated the report, you can export it in PDF, XLS, CSV, or HTML format using the **Export as** option.

▌ Summary

Every organization has unique reporting needs that can't always be met using prebuilt reports. ADManager Plus' Custom Reports feature helps overcome this challenge by providing:

- Report filters.
- Custom attribute-based reporting.
- LDAP query-based reporting.

Admins no longer have to waste their precious time downloading and manipulating every report; instead, they can build reports that match their exact requirements using ADManager Plus.

ManageEngine
ADManager Plus

ManageEngine ADManager Plus is a web-based Windows AD management and reporting solution that helps AD administrators and help desk technicians accomplish their day-to-day activities. With an intuitive, easy-to-use interface, ADManager Plus handles a variety of complex tasks and generates an exhaustive list of AD reports, some of which are essential requirements to satisfy compliance audits. It also helps administrators manage and report on their Exchange Server, Office 365, and Google Apps environments, in addition to AD, all from a single console. For more information about ADManager Plus, visit manageengine.com/ad-manager.

| $ Get Quote | ⬇ Download |