

An essential guide to create **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. ADManager Plus helps admins overcome this challenge. The Custom Reports feature allows admins to:

- Filter data to narrow their results based on their exact requirements.
- Create reports that include custom attributes in their AD.
- Build reports based on LDAP queries.
- Perform management actions from custom reports.
- 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. It can be difficult to find the information they need, even if some reports allow them to customize the fields displayed in the report. 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 using ADManager Plus, which allows admins to use filters like naming attributes, employee IDs, proxy addresses, etc. to fetch their exact requirements in a report. Create custom reports from scratch on user account expiration, user passwords, group members, and other vital information, and use them like any other report with ADManager Plus.

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. Specifically, they only want information for marketers working on five different products (A, B, C, D, and E). Since this requirement is very specific, the 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 **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:
 - a. Report name: Marketing team password reset report
 - b. 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.

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

8. In the **Filters** section,

- a. Click **LDAP Filter** to create a customized LDAP search query for an object. You can add the conditions to the filter. Select
 - When Created attribute → Before N days → 30
 - AND Password Last Set → Before N days → 30
 - AND Department Is marketing
- b. Click **Advanced Filter** to automatically update the LDAP query based on the pre-defined report chosen in the *Filter from Report* option.
- c. Select **Refine results** option and click **Add Conditions** to refine your criteria on a database level.

Refine Results

1. First Name Starts With R

2. AND Department Is Marketing

OR

3. Last Name Starts With P

4. AND Department Is Marketing

Criteria : (1 and 2 or (3 and 4))

Save Preview Query Cancel

9. Click symbol to add grouped conditions which is applicable to both **LDAP Filters** as well as **Refine Results**.

ADManager Plus

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

Filters Columns Management Actions

☐ General

☒ Display Name

☐ First Name

☐ Last Name

☐ Initials

☒ Common Name

☒ Domain Name

☐ OU Name

☐ Object Class

☐ Description

☐ Member of

☐ MemberOf Location

☐ Full Name

☐ Primary Group

☐ SID

☐ Object GUID

☐ Distinguished Name

☐ When Changed

☐ When Created

☐ Domain Controller Name

☐ PSO Applied

☐ PSO Resultant

☐ Account

☒ SAM Account Name

☐ Logon Name

☐ Password Status

☐ Password Last Set

☐ Password Expiry Date

☐ Account Expiry Time

☐ Last Logon Time

☐ Days Since Last Logon

☐ Account Status

☐ Password expires in

☐ Profile Path

☐ Bad Password Time

☐ Bad Password Count

☐ User Logon Count

☐ Logon To

☐ Home Directory

☐ Script Path

☐ Lockout Time

☐ Days since password last set

☐ Pwd Never Expires Flag

☐ Last Logon Time Stamp

☐ Smart Card

☐ User Account Control

☐ User Account Control Flag

☐ Contact

☐ Email Address

☐ Manager

☐ Title

☐ Department

☐ Company

☐ Employee ID

☐ Employee Number

☐ Telephone Number

☐ Notes

☐ City

☐ Street Address

☐ State/Province

☐ Zip Code

☐ Country

☐ Home Phone

☐ Pager

☐ Mobile

☐ Fax

☐ IP Phone

☐ Web Page

☐ Office

☐ Exchange

☐ E-mail Alias

☐ Simple Display name

☐ Mailbox Store

☐ Proxy Addresses

☐ External e-mail addresses

☐ Recipient limit

☐ Home Mail Server

☐ Sending Message Size (KB)

☐ Receiving Message Size (KB)

☐ Accept messages from authenticated users only

☐ Reject messages from

☐ Accept messages from

☐ Send on behalf

☐ Forward to

☐ Deliver and Redirect

☐ Warn at message size (KB)

☐ Prohibit message sending at (KB)

☐ Prohibit send and receive messages at (KB)

☐ Is hidden to address lists

☐ Outlook Mobile Access

☐ Outlook Web Access

☐ IMAP4 Protocol

☐ POP3 Protocol

Select custom attributes

Save Preview Query Cancel

10. Select the **Column** option to specify the columns that must be shown in the resulting report. Select the management actions that can be performed, directly from the custom report.

11. Click **Save**.

12. Now that you've created the report, you can export it in **PDF, XLS, CSV, CSVDE, 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 AD 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.

In such cases, a custom report where the filter conditions are set using custom attributes can be generated from scratch, or in the final report of select objects (viz., users, groups, computer and contact). Custom attributes can be added in filter conditions to get updated reports from the original reports.

Use case: An organization wants to generate a series of reports based on the values of specific schema attributes, including their custom attribute and technicalteam attribute 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. They can either create a new custom report with the above mentioned attributes or include the custom attributes in the filter conditions to get updated reports instantaneously. 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 AD attributes 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:

Add report to:

Select domains: ☒ admpdev.com Selected OUs: All [Add OUs](#) ☒ csez.zohocorpin.com Selected OUs: All [Add OUs](#)

Description: A report to generate the list of Marketing team members of five different products (A, B, C, D, and E)

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**.

Refine Results

1. First Name Starts With R

2. AND Department Is Marketing

OR

3. Last Name Starts With P

4. AND Department Is Marketing

Criteria : (1 and 2 or (3 and 4))

[Save](#) [Preview Query](#) [Cancel](#)

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

Select custom attributes

General	Account	Contact	Exchange
<input checked="" type="checkbox"/> Display Name	<input checked="" type="checkbox"/> SAM Account Name	<input type="checkbox"/> Email Address	<input type="checkbox"/> E-mail Alias
<input type="checkbox"/> First Name	<input type="checkbox"/> Logon Name	<input type="checkbox"/> Manager	<input type="checkbox"/> Simple Display name
<input type="checkbox"/> Last Name	<input type="checkbox"/> Password Status	<input type="checkbox"/> Title	<input type="checkbox"/> Mailbox Store
<input type="checkbox"/> Initials	<input type="checkbox"/> Password Last Set	<input type="checkbox"/> Department	<input type="checkbox"/> Proxy Addresses
<input checked="" type="checkbox"/> Common Name	<input type="checkbox"/> Password Expiry Date	<input type="checkbox"/> Company	<input type="checkbox"/> External e-mail addresses
<input checked="" type="checkbox"/> Domain Name	<input type="checkbox"/> Account Expiry Time	<input type="checkbox"/> Employee ID	<input type="checkbox"/> Recipient limit
<input type="checkbox"/> OU Name	<input type="checkbox"/> Last Logon Time	<input type="checkbox"/> Employee Number	<input type="checkbox"/> Home Mail Server
<input type="checkbox"/> Object Class	<input type="checkbox"/> Days Since Last Logon	<input type="checkbox"/> Telephone Number	<input type="checkbox"/> Sending Message Size (KB)
<input type="checkbox"/> Description	<input type="checkbox"/> Account Status	<input type="checkbox"/> Notes	<input type="checkbox"/> Receiving Message Size (KB)
<input type="checkbox"/> Member of	<input type="checkbox"/> Password expires in	<input type="checkbox"/> City	<input type="checkbox"/> Accept messages from authenticated users only
<input type="checkbox"/> MemberOf Location	<input type="checkbox"/> Profile Path	<input type="checkbox"/> Street Address	<input type="checkbox"/> Reject messages from
<input type="checkbox"/> Full Name	<input type="checkbox"/> Bad Password Time	<input type="checkbox"/> State/Province	<input type="checkbox"/> Accept messages from
<input type="checkbox"/> Primary Group	<input type="checkbox"/> Bad Password Count	<input type="checkbox"/> Zip Code	<input type="checkbox"/> Send on behalf
<input type="checkbox"/> SID	<input type="checkbox"/> User Logon Count	<input type="checkbox"/> Country	<input type="checkbox"/> Forward to
<input type="checkbox"/> Object GUID	<input type="checkbox"/> Logon To	<input type="checkbox"/> Home Phone	<input type="checkbox"/> Deliver and Redirect
<input type="checkbox"/> Distinguished Name	<input type="checkbox"/> Home Directory	<input type="checkbox"/> Paper	<input type="checkbox"/> Warn at message size (KB)
<input type="checkbox"/> When Changed	<input type="checkbox"/> Script Path	<input type="checkbox"/> Mobile	<input type="checkbox"/> Prohibit message sending at (KB)
<input type="checkbox"/> When Created	<input type="checkbox"/> Lockout Time	<input type="checkbox"/> Fax	<input type="checkbox"/> Prohibit send and receive messages at (KB)
<input type="checkbox"/> Domain Controller Name	<input type="checkbox"/> Days since password last set	<input type="checkbox"/> IP Phone	<input type="checkbox"/> To hidden to address lists
<input type="checkbox"/> PSO Applied	<input type="checkbox"/> Pwd Never Expires Flag	<input type="checkbox"/> Web Page	<input type="checkbox"/> Outlook Mobile Access
<input type="checkbox"/> PSO Resultant	<input type="checkbox"/> Last Logon Time Stamp	<input type="checkbox"/> Office	<input type="checkbox"/> Outlook Web Access
	<input type="checkbox"/> Smart Card		<input type="checkbox"/> IMAP4 Protocol
	<input type="checkbox"/> User Account Control		<input type="checkbox"/> POP3 Protocol
	<input type="checkbox"/> User Account Control Flag		

[Show less](#)

[Save](#) [Preview Query](#) [Cancel](#)

You will be redirected to the Admin tab to create custom attribute, where you can create the attribute to suit your needs. Once it is created, it will be reflected under the 'Configured Custom Attribute'.

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: Description: A report to generate last logon time and password expiry details of the Networking team.

Add report to:

Select domains: ☒ admpdev.com Selected OUs: All [Add OUs](#) ☒ csez.zohocorp.in Selected OUs: All [Add OUs](#)

Conditions: **Users** +

LDAP Filter

1.

Criteria : (1)

[Advanced Filter](#)

Preview Query: (&(&(objectCategory=person)(objectClass=user))((extensionAttribute1=Networking)))

[Refine Results](#)

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)))

Custom Report

Report name: Description: A report to generate last logon time and password expiry details of the Networking team.

Add report to:

Select domains: ☒ admpdev.com Selected OUs: All [Add OUs](#) ☒ csez.zohocorp.in Selected OUs: All [Add OUs](#)

Conditions: **Users** +

LDAP Filter

1.

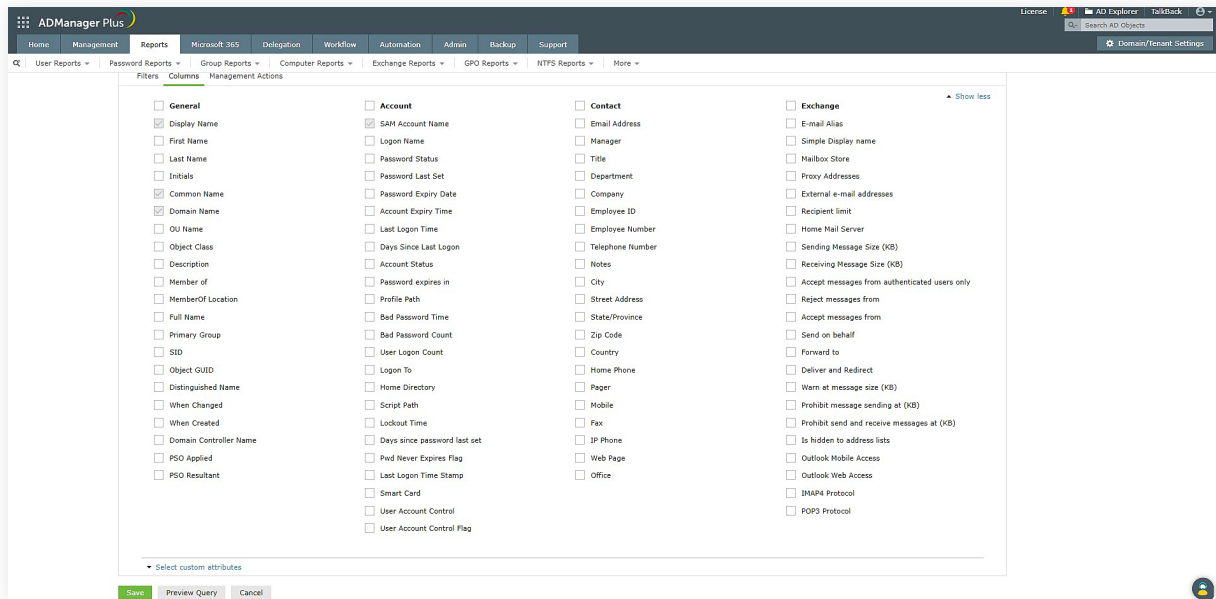
Criteria : (1)


[Advanced Filter](#)

Preview Query: (&(&(objectCategory=person)(objectClass=user))((extensionAttribute1=Networking)))

[Refine Results](#)

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 **LDAP Filters**, and add the conditions based on the report you want. If you want to add nested conditions like (1 AND 2 OR (3 AND 4)) click the  symbol. You can frame these conditions based on your needs.
11. Click **Save**
12. 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.

Our Products

AD360 | Log360 | ADAudit Plus | ADSelfService Plus | M365 Manager Plus | RecoveryManager Plus

ManageEngine 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 Azure AD management.

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

\$ Get Quote

↓ Download