ManageEngine
ADManager Plus

Integrating HCM applications

with ADManager Plus

Integrating HCM applications with ADManager Plus

Human capital management (HCM) enables organizations to plan and implement different administrative functions of human resources, such as compensation, payroll, performance management, and recruiting as opportunities that increase productivity, and drive engagement.

Organizations still have to depend on IT teams to provision and deprovision user accounts. This technical guide illustrates how integrating HCM applications with MangeEngine ADManager Plus can eliminate the dependency on other teams and promote better employee onboarding experience.

Integrating your HCM solution with ADManager Plus automates AD user account management operations. ADManager Plus supports integration with any HCM application through API endpoints.

Supported features:

Feature	Description
User provisioning	New employee accounts created in the HCM solution automatically generates new user identities in AD.
Modify user details	Changes made to the user attributes configured in the HCM are automatically updated in AD.
User deprovisioning	Deleting the employee details as and when they move out of the organization automatically deletes the user accounts in AD.

Prerequisites:

1. The HCM solution should have a proper REST API which will fetch all the employee information in a JSON format.

2. The type of authorization used for the endpoints by your HCM solution should be one of the following: Basic Auth, OAuth 2.0 (grant type must be authorization code), Bearer, or just an API key.

Configuration steps:

1. Log into ADManager Plus as an Administrator. Navigate to the **Automation** tab and click **HCM Integrations.**

2. Under HCM, click on the **Custom HCM** tile to integrate a new custom HCM solution.

3. In the Custom HCM Integration window that displays, enter a suitable **Name**, **Description,** upload a **Logo** of the HCM solution, and hit **Save.**

4. Click on the custom HCM solution logo added in the previous step to configure the API authorization methods (API key, Basic Authentication, Bearer, OAuth 2.0), endpoints and LDAP data mapping.

5. In the Authorization section, select the **Authorization Type** required for the endpoint to be configured from the drop-down, and select the appropriate option.

No Auth

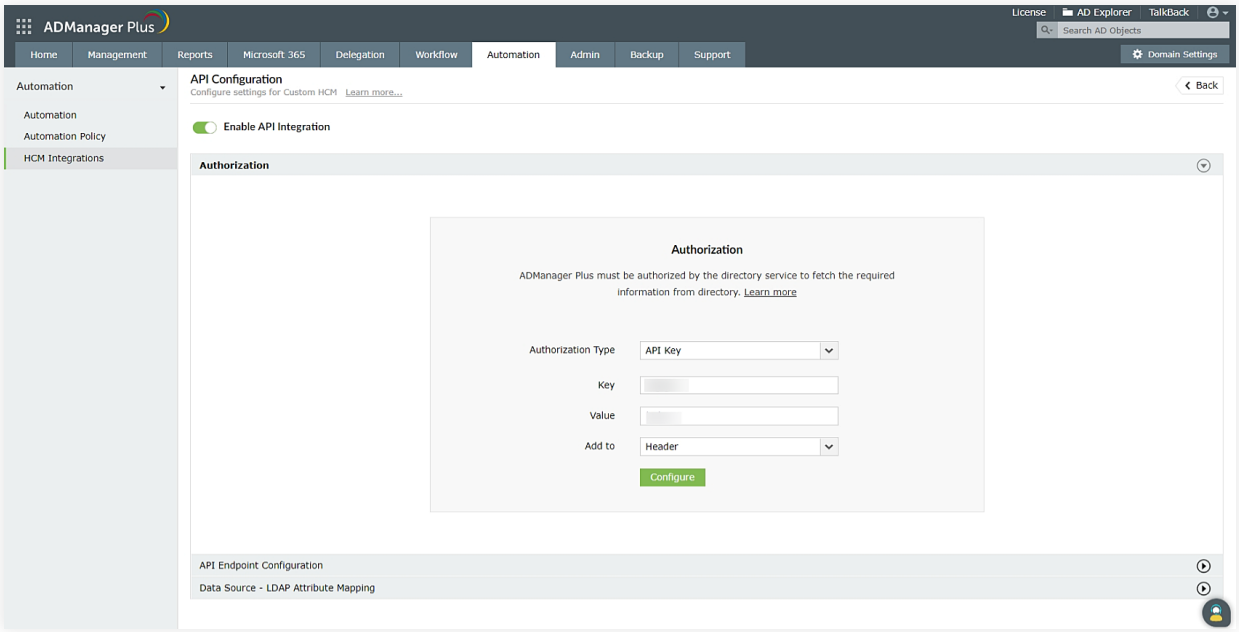
Select No Auth as the authorization type, if you prefer to add authorization details manually during endpoint configuration. Click on **Configure.**

API Key

If you select API key as the authorization type,

i. Enter the key name and value fetched from the HCM solution in the **Key** and **Value** fields respectively.

ii. Associate the key to a header or query parameter using the **Add To** drop down menu and click **Configure.**

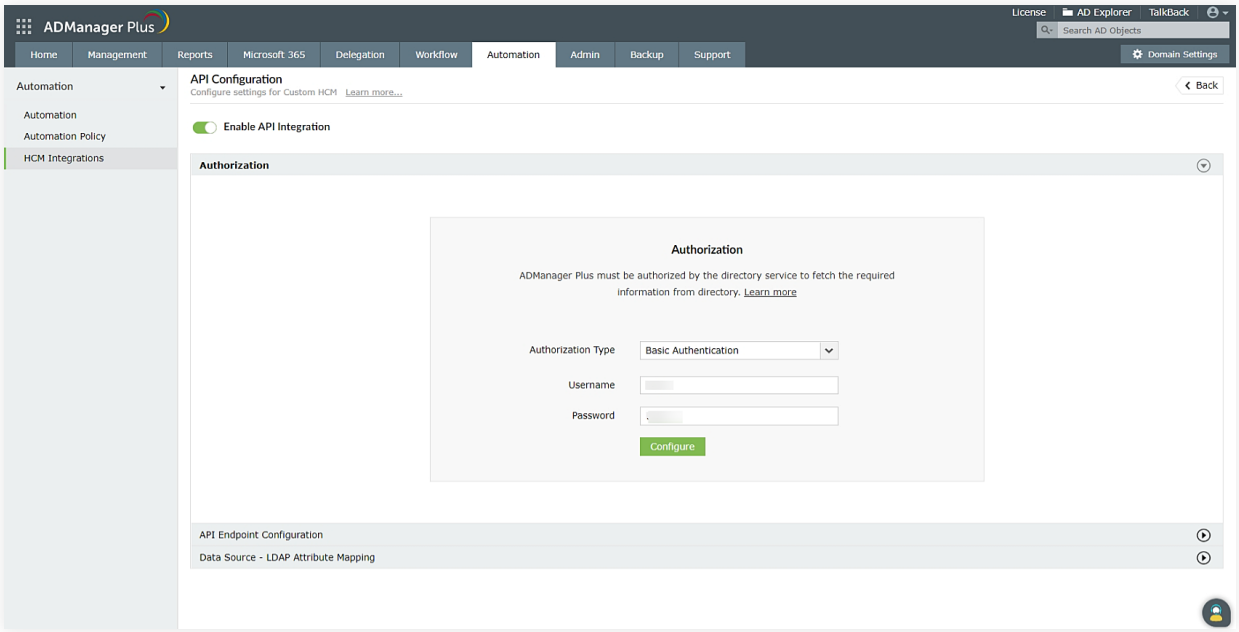


Basic Authentication

If you select Basic Authentication as the authorization type,

i. Specify the **Username** and **Password** configured in your HCM solution,

ii. Click **Configure.**

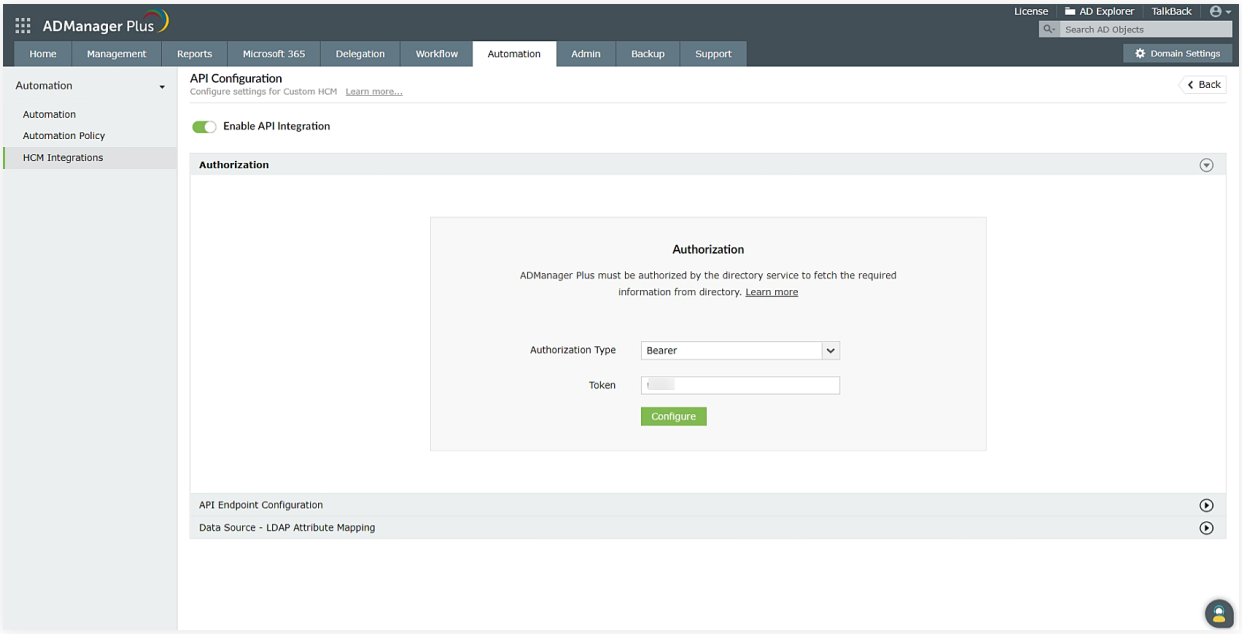


Bearer

If you select Bearer as the authorization type,

i. Enter your API key fetched from the HCM solution in the **Token** field

ii. Click **Configure.**



OAuth 2.0

If you select OAuth 2.0 as the authorization type, specify the following:

i. **Header Prefix:** Specify a prefix value for your authorization header.

OAuth 2.0 Grant Type: authorization code is the default grant type.

Callback URL: The Callback URL is where you will be redirected to after authentication. This should be registered with the API provider.

Auth URL: Specify the Authorization Endpoint URL.

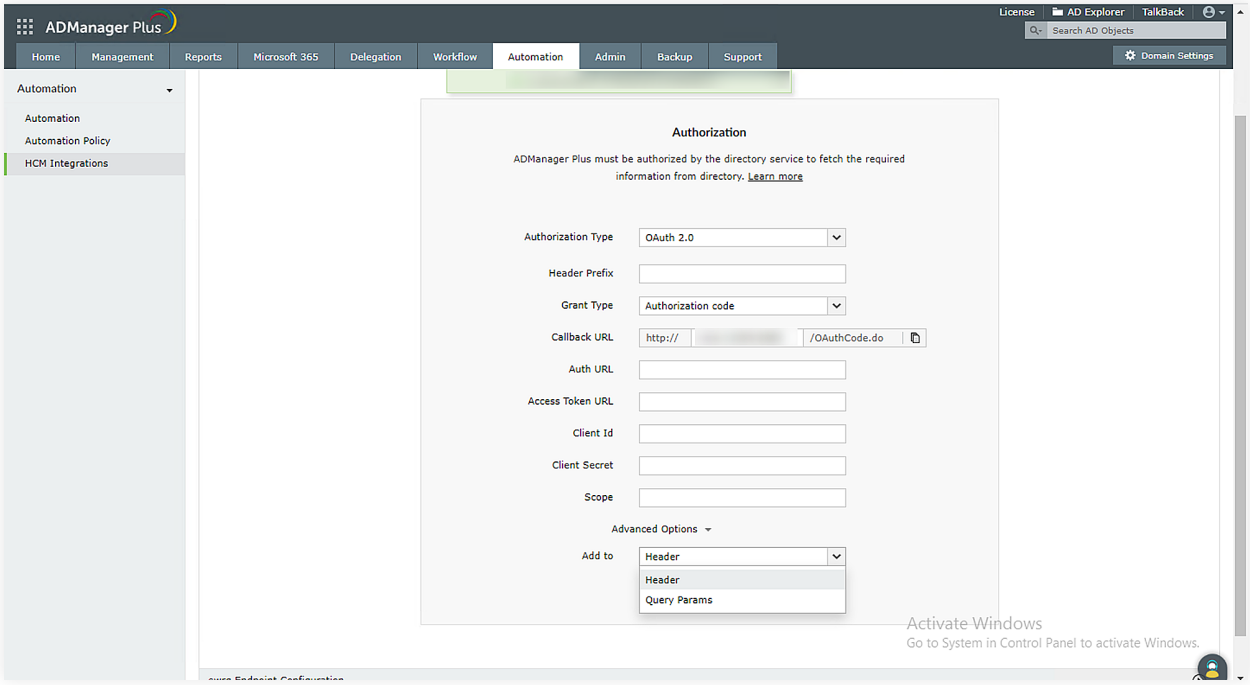
Access Token URL: Enter the OAuth server URL where the application can exchange the authorization code for an access Token.

Client Id and Client Secret: Enter a valid ID and its secret key.

Scope: Specify the data you would like to access.

ii. Click **Advanced Options** and choose the Header and Query Params from the Add To drop-down menu.

Note: To know when to choose Header and Query Params for OAuth2.0/API key in the **Add to field**, refer to the API documentation of the HCM solution.



ADManager Plus sends an authorization request to the Auth URL specified above along with the Client Id. The authorization server will prompt for login and after successful authorization, redirects to callback URL with an authorization code, which is then exchanged for refresh and access Tokens.

6. In the API Endpoint Configuration section, add the following:

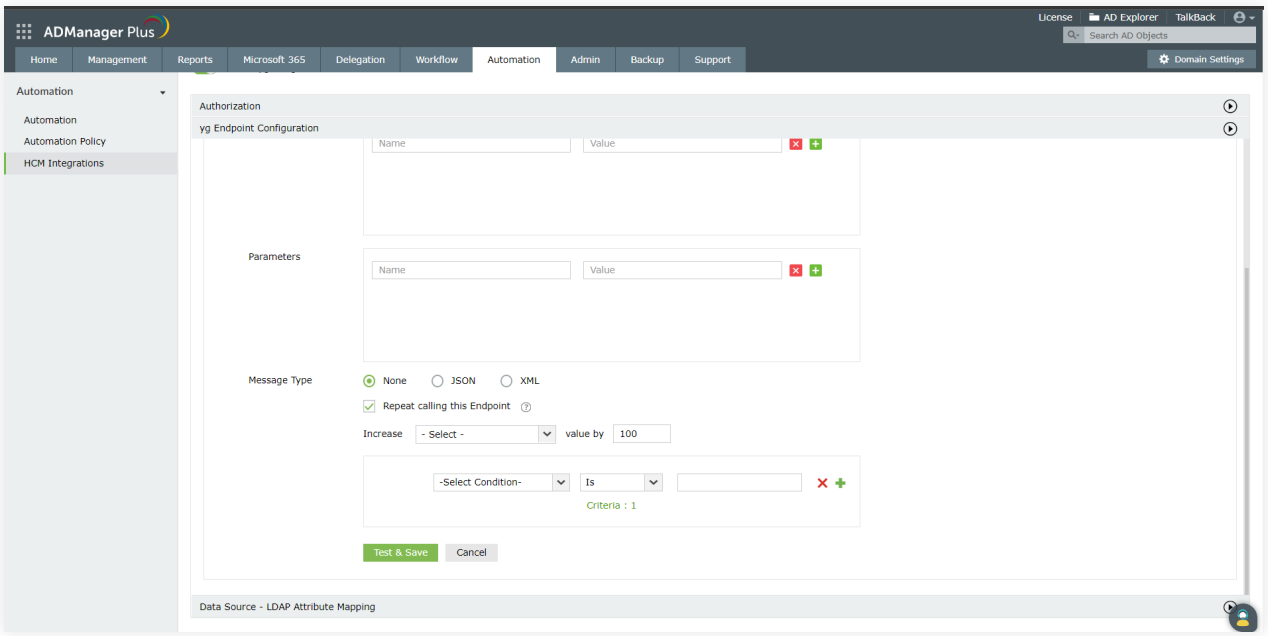
   i. **Endpoint URL:** Enter the Endpoint URL.

   ii. Click **Advanced Options** to add headers and parameters.

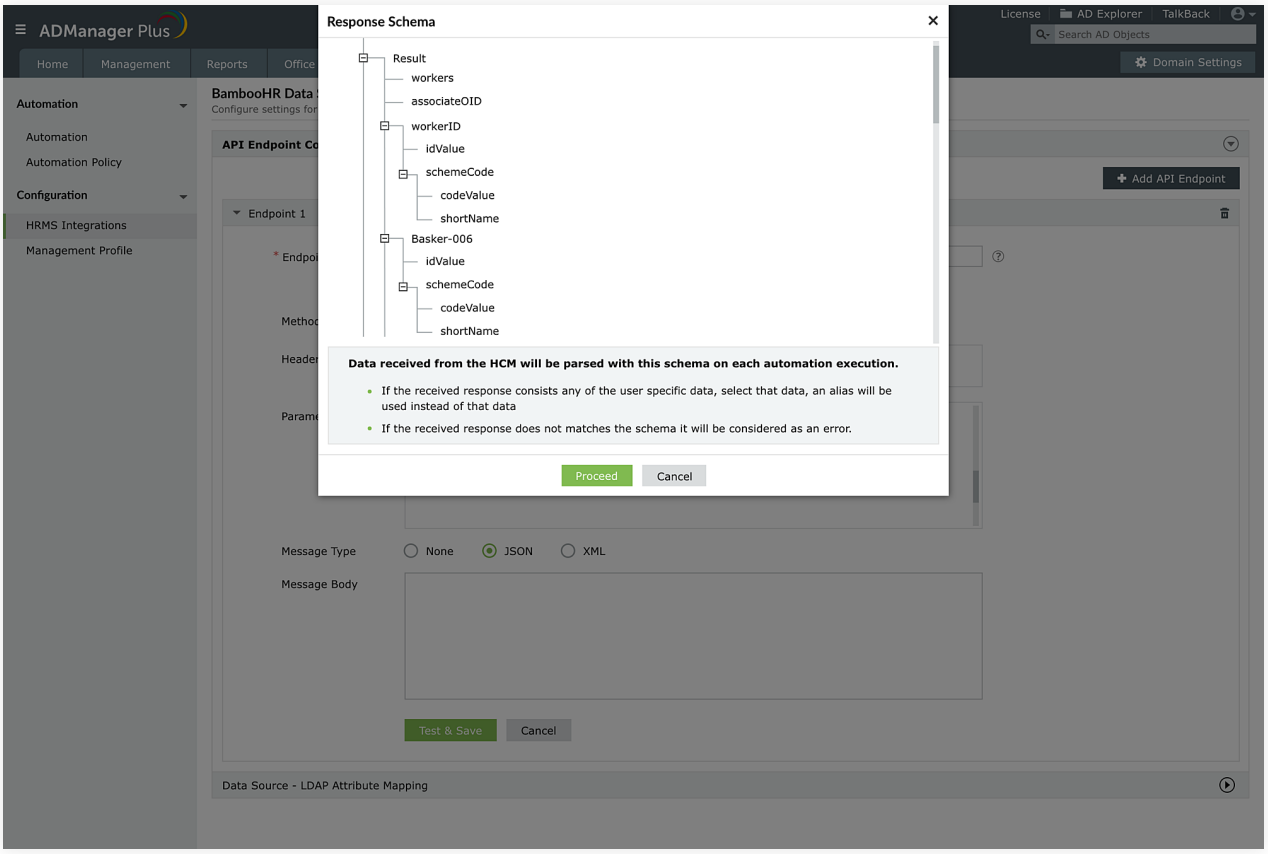
   - **Method:** Choose between the HTTP request methods **Get** and **Post.**
   - **Headers:** Click and configure the respective HTTP headers.
   - **Parameters:** Cick and configure the query parameters.
   - **Message type:** The default message type will be **None.** If you want to add a message body then select the appropriate message type (JSON or XML).

If your HCM tool has a limitation on the maximum number of users per API request, check the **Repeat calling this Endpoint option.** For example, if your REST API follows pagination, the iteration happens based on the page count. You can select the parameter "Page" to be iterated and increase the iteration value by "1". Construct a condition from the following options based on which the endpoint should repeatedly be called:

- **Until a response:** Use this condition when you know the details of the response on the last page received from the HCM.
- **Up to a parameter value:** Create this condition to mention the parameter name (e.g., total_page). The parameter's value is used to iterate the API call.
- **Up to N time:** Create this condition when you want to repeatedly call the API endpoint up to a particular integer value.

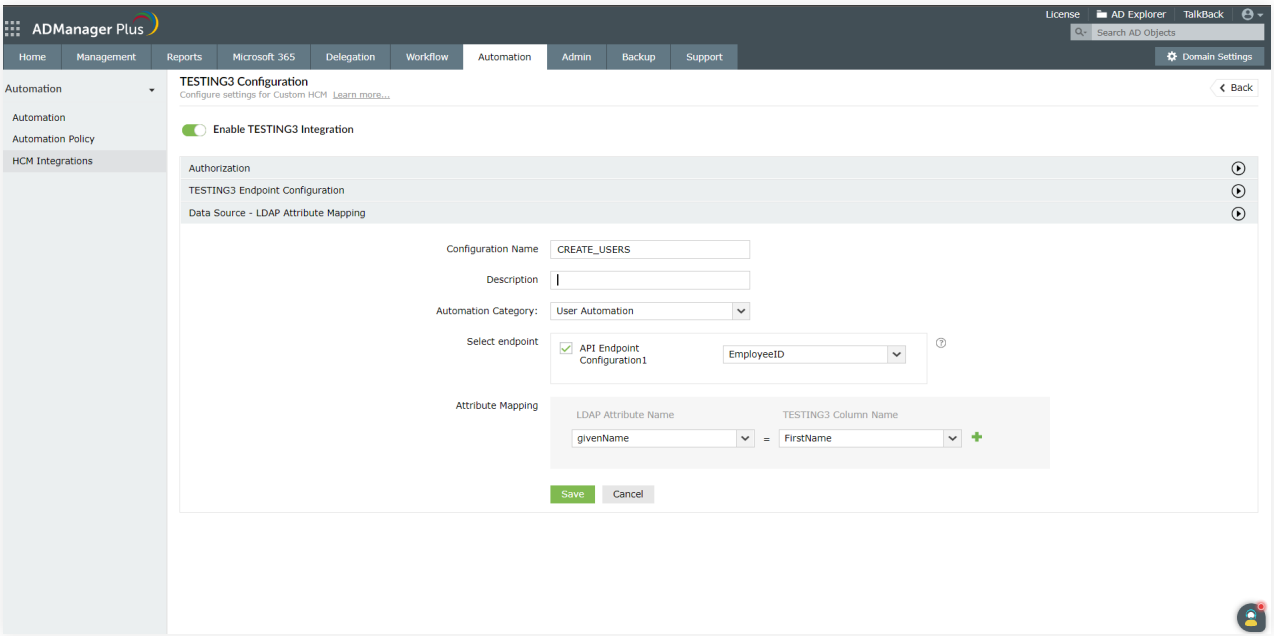


7. Once done, click **Test & Save.** A response window will display all the requested elements. Check if the received response from the HCM matches the response schema, click on **Proceed** to save the configuration.



Note: Clicking **Test & Save** will display the response schema window shown above. If you do not see the response window after clicking on **Test & Save,** go through the API documentation of your HCM solution to check for the values entered. If you've followed the API documentation and still don't see the response schema window, contact us.

8. Click **Data Source - LDAP Attribute Mapping** to map AD LDAP attributes with the respective attributes received from the the HCM solution.



9. Enter the **Configuration Name** and **Description.** Select the **Automation Category** (that currently supports user and group automation alone) from the drop-down menu.

10. Select all the endpoints that needs to be used for LDAP attribute mapping in the **Select Endpoint** field, and from the drop-down menu select the unique attributes for the endpoints selected (EmployeeID, username, etc.)

11. In the **Attribute Mapping field,** select the attribute from the HCM solution and map it with the corresponding LDAP attributes.

12. Click **Save.**

Note: While configuring an automation, select the custom HCM created as the Data Source and automate user management activities. Click here to learn more about automation configuration.

You have now integrated your HCM with ADManager Plus.

Note: In case your HCM solutions gets data from multiple endpoints, you can configure it by clicking on **+Add API Endpoint.**

What's next? Configure automations to modify and delete user accounts in AD or add users to groups based on the changes made to the corresponding employee records in the HCM solution.Now every time an employee record is added to the HCM solution, a user account for that employee will be created in AD.

For further assistance contact us here.

ManageEngine
ADManager Plus

ADManager Plus is a unified management and reporting solution for Active Directory, Microsoft 365, Exchange, and Google Workspace. The solution offers more than 200 out-of-the-box, actionable reports that fetch vital data across multiple platforms. With its help desk delegation capability, admins can define roles and delegate tasks securely to non-admin users. Other capabilities of ADManager Plus include file permissions management, automated stale account cleanup, GPO management, and customizable workflows. Admins can also manage Active Directory on-the-go with iOS and Android apps.
For more information about ADManager Plus, visit
https://www.manageengine.com/products/ad-manager/

$ Get Quote Download