Access certification use-cases

The following are a few use cases that will demonstrate sample scenarios for using access certification feature.

1. **Automatic reviewing of vendor and contractor access to resources.**
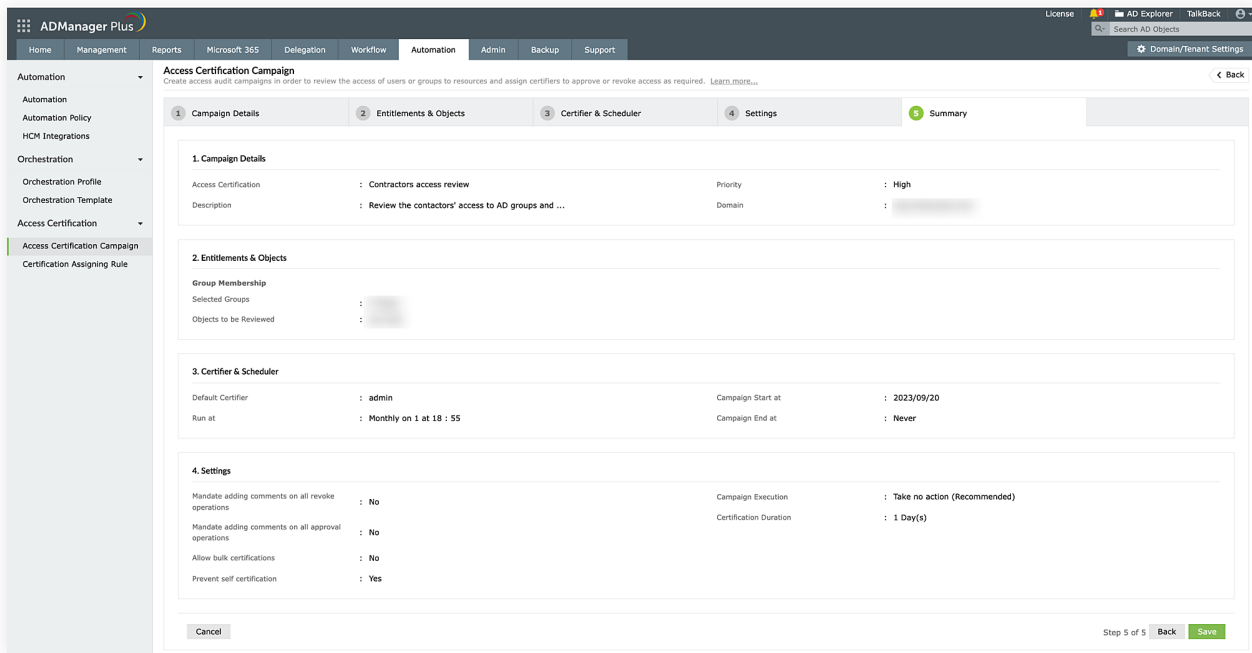2. **User access review following changes in job roles.**

Use case : 1

Automatic reviewing of vendor and contractor access to resources

It is very common for organizations to have vendors or contractors that are given temporary access to enterprise systems. ADManager Plus' automated access certification campaigns help monitor and review their permissions at specified intervals to ensure they can only access what is necessary for their tasks and only for the duration they require.

Steps to configure this access certification campaign:

1. Navigate to **Automation → Access Certification → Access Certification Campaign.**
2. The resulting page will show all the existing campaigns and their details. To create a new campaign, click on **Create New Campaign** on the top-right corner.
3. Under **Campaign Details** tab, provide the below details:
   - **Certification Campaign Name:** Contractors access review
   - **Description:** Review the contactors' access to AD groups and revoke if not needed
   - **Priority:** High
   - **Select Domain:** Domain in which the campaign must be run.
4. Once all the above details are entered, click **Next.**
5. Under **Entitlements & Objects**, specify the below details:
   - In the *Entitlement Selection* section, toggle the button beside *Group Membership* and select the group(s) to be reviewed.
   - In the *Object Selection* section, select **User** and choose the filter mentioned below,
     - **Select User(s):** Manually choose the contractors names that need to be reviewed.

6. After completing all the above steps, click **Next.**

7. In the **Certifier & Scheduler** tab, within the *Certifier* section, select a **Default Certifier** or choose an certifier assigning rule to assign a technician dynamically. Click here to learn how to create a certifier assigning rule.

8. In the Scheduler section, you can define the following details:

   - **Start Date:** Specify the current date.
   - **Run at:** Specify the frequency at which the campaign must be run. Here you can choose the campaign to be run on the 1st of every month at 10am.
   - **End:** Select **Never** to keep the campaign running indefinitely.

9. Click Next.

10. Under **Settings** tab, you can select **Mandate adding comments on all revoke operations** in the *Configuration* section.

11. In the *Campaign Settings* section, you can define the below actions:

   - **Certification Request Expiration:** Configure as 1 week
     - Select **Send reminder to certifiers** and configure notifications to be sent everyday, continuously after 1 day of request creation.
   - **Campaign Execution:** You can select a default action to be performed when the certifier has not approved or revoked an access request. You can select **Take no action (Recommended).**

12. Click **Next** and view the summary of the campaign created.

Use case : 2

User access review following changes in job roles

Real-time access certification can be used to verify access rights when an employee's role changes or they switch teams. If an employee is assigned a new role with different access requirements, the campaign ensures they hold the appropriate permissions as required.

Steps to configure this access certification campaign:

1. Navigate to **Automation → Access Certification → Access Certification Campaign.**

2. The resulting page will show all the existing campaigns and their details. To create a new campaign, click on **Create New Campaign** at the top-right corner.

3. Under **Campaign Details** tab, provide the below details:
   - **Certification Campaign Name:** Role change access review
   - **Description:** Review the access to AD groups and revoke if not needed
   - **Priority:** High
   - **Select Domain:** Domain in which the campaign must be run

4. Once all the above details are entered, click **Next.**

5. Under **Entitlements & Objects**, specify the below details:
   - In the *Entitlement Selection* section, toggle the button beside *Group Membership* and select the group(s) to which the user has access that needs to be reviewed.

- In the *Object Selection section*, select **User** and choose either of the following filters:
  - **Select User(s):** Manually select the user names whose access needs to be reviewed.

    (or)

  - **Select from Report:** Select AD group members report and customize it to fit your criteria by setting up filter conditions.

6. After completing all the above steps, click **Next.**

7. In the **Certifier & Scheduler** tab, within the *Certifier* section, select a **Default Certifier** or choose an certifier assigning rule to assign a technician dynamically. Click here to learn how to create a certifier assigning rule.

8. In the *Scheduler* section, you can define the following details:
   - **Start Date:** Specify the current date.
   - **Run at:** Specify the frequency at which the campaign must be run. Here you can choose the campaign to be run on the 1st of every month at 10am.
   - **End:** Select **Never** to keep the campaign running indefinitely.

9. Click **Next.**

10. Under the **Settings** tab, you can select **Mandate adding comments on all approve or revoke operations** in the *Configuration* section.

11. In the *Campaign* Settings section, you can define the below actions:
    - **Certification Request Expiration:** Choose when the request should expire.
      - Select **Send reminder to certifiers** and configure notifications to be sent everyday, continuously after 1 day of request creation.
    - **Campaign Execution:** Select a default action to be performed when the certifier has not approved or revoked an access request. You can select **Take no action (Recommended).**

12. Click **Next** and view the summary of the campaign created.

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