ManageEngine
ADManager Plus

ADManager Plus Access Certification Campaign

Preventing privilege creep and meeting compliance requirements

→

Imagine a world where managing user access is streamlined and efficient. With today's digital security demands, wouldn't it be amazing to have a structured process that guarantees the right access for every user?

ADManager Plus' access certification campaigns offer a structured process to ensure the rights and privileges assigned to users are accurate and up-to-date

Why do organizations need access certification campaigns?

Mitigate access-related risks

By regularly reviewing and certifying access rights, organizations can demonstrate compliance with regulatory requirements and industry standards, avoiding penalties and legal consequences

Ensure compliance

Access certification campaigns ensure that access rights align with organizational policies, reducing the risk of unauthorized access and potential security breaches

ADManager Plus'
Access Certification Campaign

- ✓ An access certification campaign is a process that involves **reviewing and validating users' access rights and privileges**

- ✓ Access certification campaigns can be utilized to **recertify and revoke users' access rights** and implement the principle of least privilege and role-based access control

- ✓ With the access certification campaigns in ADManager Plus, **user access rights can be validated in bulk**, resulting in improved operational efficiency

ManageEngine
ADManager Plus

Components of access certification campaign

Certification campaigns

Audit campaigns that can be scheduled and prioritized according to the entitlements to be assessed

Entitlements

Users' group memberships and access permissions that will be validated by the certifier

Certifier assigning rules

Rules that can be configured to dynamically assign certifiers for the audit campaigns

Certifier

A key stakeholder in the procedure responsible for reviewing and managing users' access permissions. The role of a certifier may be fulfilled by an administrator, help desk technician, a user's manager, or tailored according to the organization’s requirements

Campaign creation

The campaign creation process in ADManager Plus involves defining the campaign details, selecting the entitlements and objects for review, choosing certifiers and scheduling the campaign, configuring settings, and reviewing the summary of the campaign settings

STEP 1

Describe the campaign details

STEP 2

Specify the entitlements and objects to be reviewed

STEP 3

Assign certifiers and schedule the campaign

STEP 4

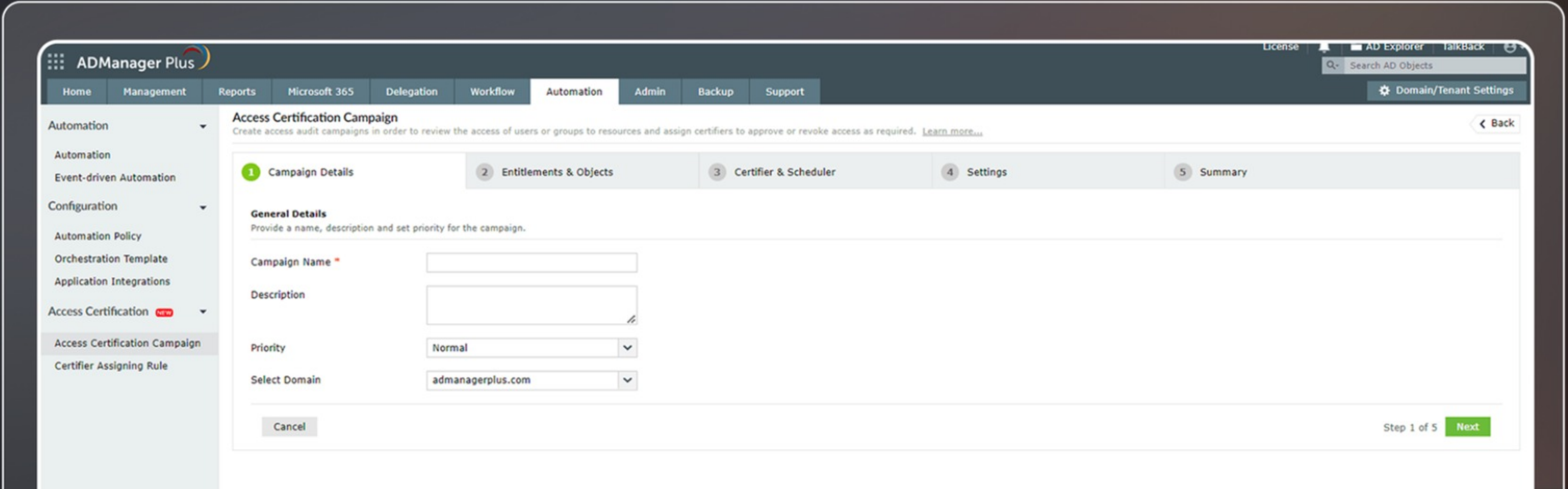
Configure custom settings for the campaign

STEP 5

View the summary of the campaign

Campaign details

Set the name, purpose, and priority for the campaign



Access Certification Campaign

Create access audit campaigns in order to review the access of users or groups to resources and assign certifiers to approve or revoke access as required. Learn more...

General Details

Provide a name, description and set priority for the campaign.

Campaign Name *	
Description	
Priority	Normal
Select Domain	admanagerplus.com

Entitlements supported

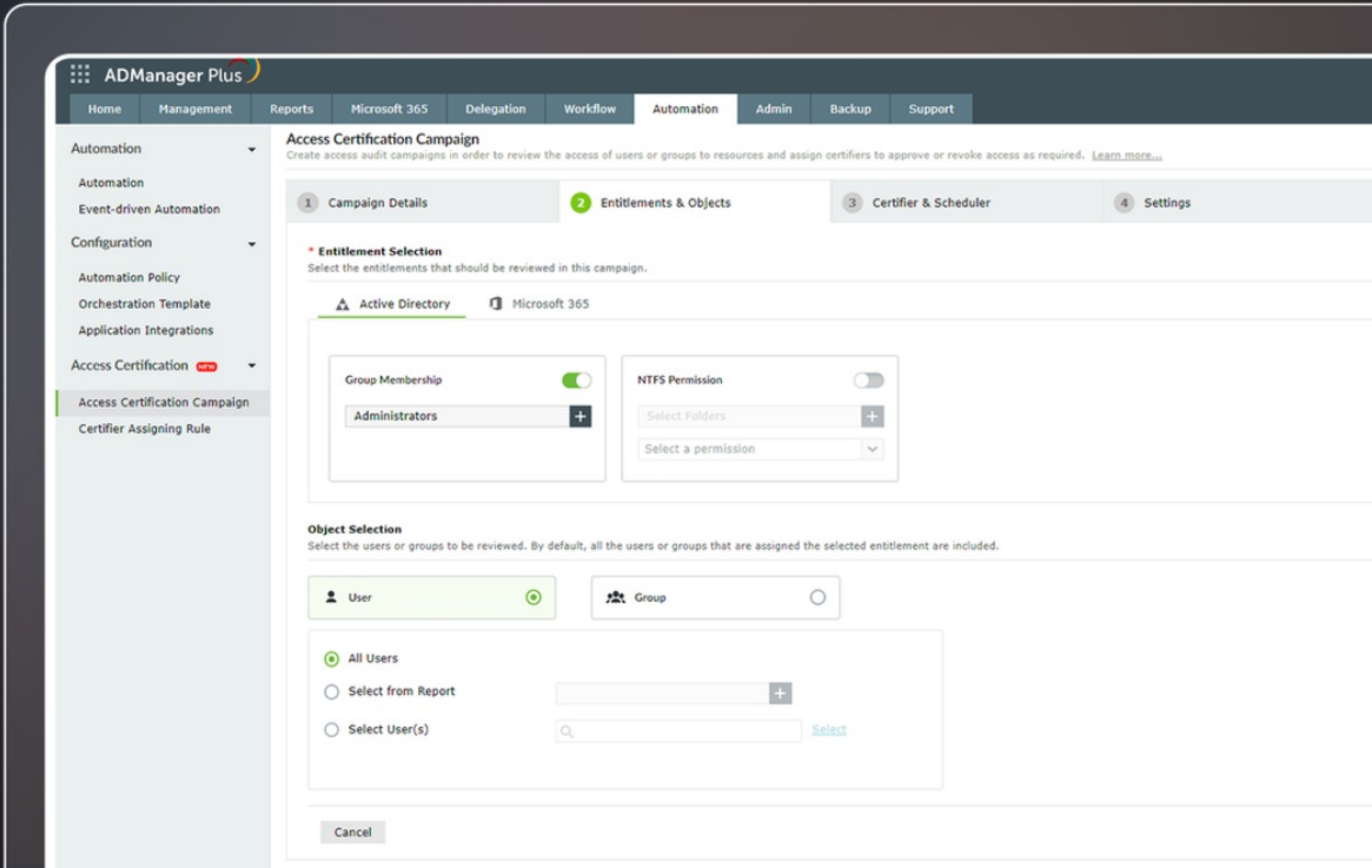
ADManager Plus allows you to review the following entitlements:

AD entitlements

- Group memberships
- NTFS permissions

Microsoft 365 entitlements

- Group memberships
- Role assignments
- Application assignments



Access Certification Campaign

Create access audit campaigns in order to review the access of users or groups to resources and assign certifiers to approve or revoke access as required. Learn more...

1 Campaign Details | 2 Entitlements & Objects | 3 Certifier & Scheduler | 4 Settings

* **Entitlement Selection**

Select the entitlements that should be reviewed in this campaign.

Active Directory | Microsoft 365

Group Membership: on
Administrators +

NTFS Permission: off
Select Folders +
Select a permission

Object Selection

Select the users or groups to be reviewed. By default, all the users or groups that are assigned the selected entitlement are included.

● User ○ Group

● All Users
○ Select from Report +
○ Select User(s) Select

Cancel

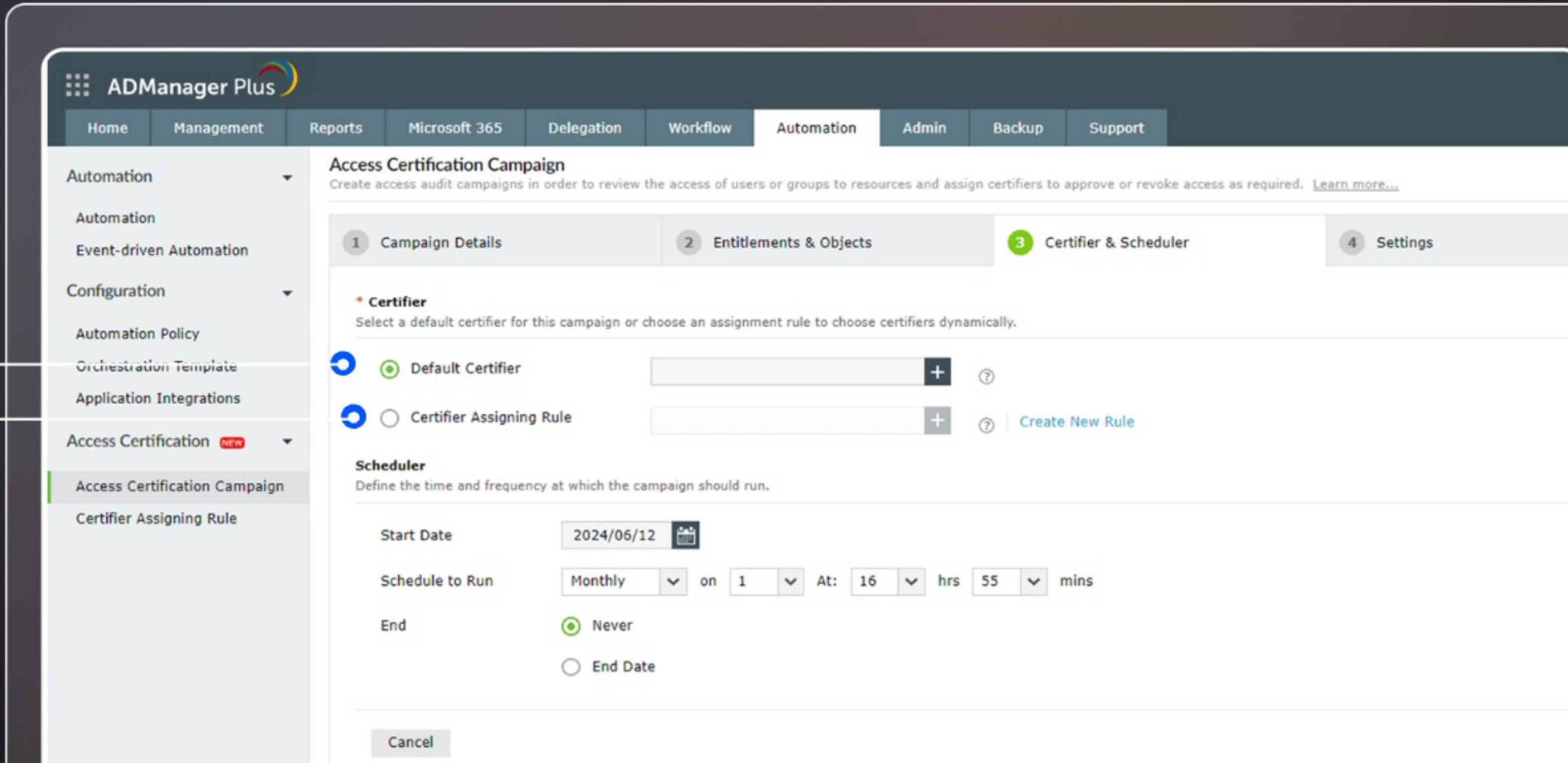
ManageEngine
ADManager Plus

Assigning a certifier

Select a certifier for the campaign and schedule the process to run automatically

You can select any one of the technicians as certifiers to review the access request and they will be assigned by default once the task is created

You can schedule the campaign to run automatically at preferred intervals (i.e., weekly, monthly, quarterly, semi-annually, annually)



Access Certification Campaign

Create access audit campaigns in order to review the access of users or groups to resources and assign certifiers to approve or revoke access as required. Learn more...

* **Certifier**

Select a default certifier for this campaign or choose an assignment rule to choose certifiers dynamically.

● Default Certifier

○ Certifier Assigning Rule

Scheduler

Define the time and frequency at which the campaign should run.

Start Date: 2024/06/12

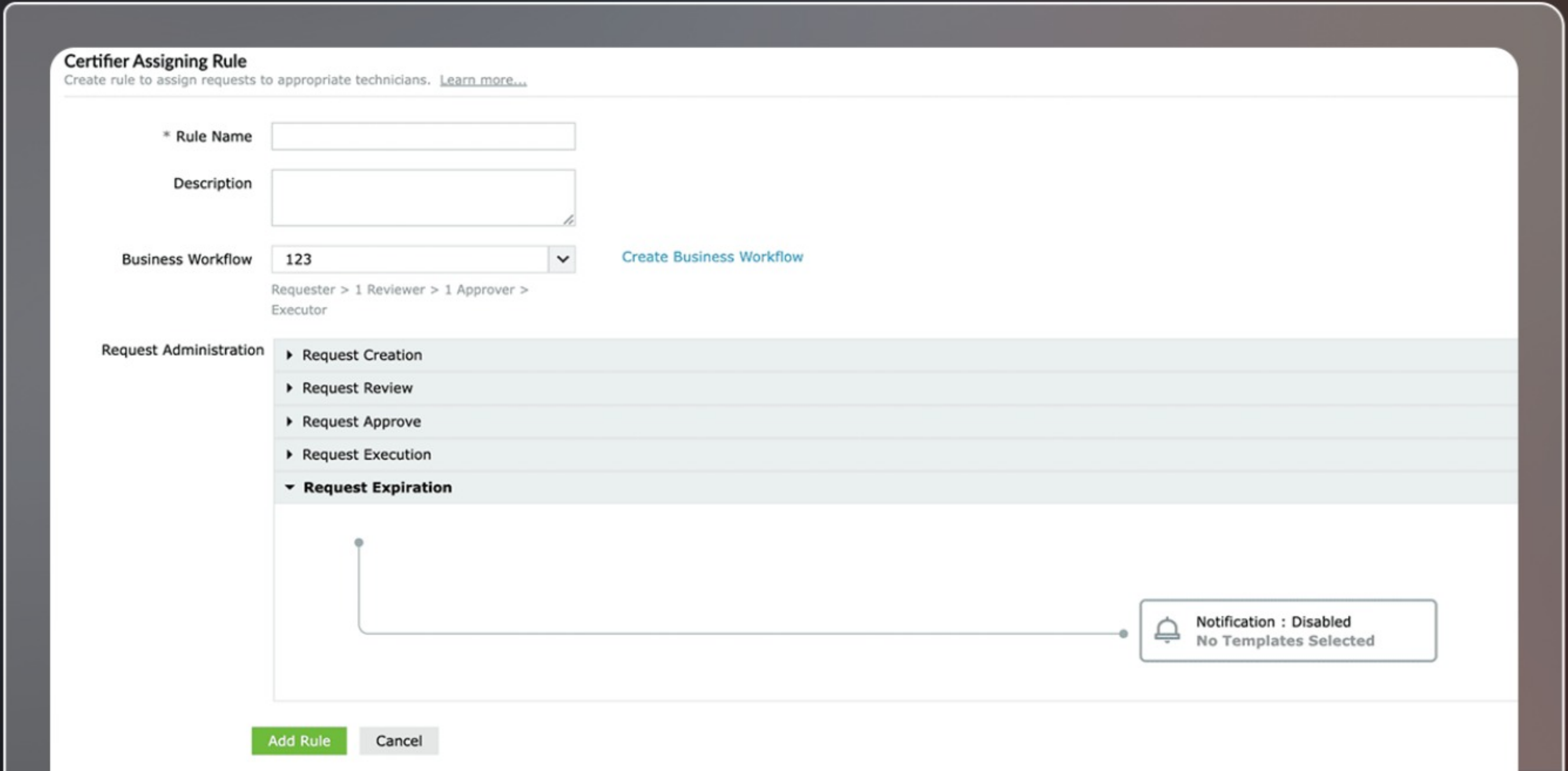
Schedule to Run: Monthly on 1 At: 16 hrs 55 mins

End: ● Never ○ End Date

ManageEngine
ADManager Plus

Certifier Assigning Rule

- ✓ The Certifier Assigning Rule will dynamically assign technicians as certifiers for access review campaigns based on the conditions specified
- ✓ Admins can also configure a workflow with reviewers, approvers, and executors through which the requests need to be reviewed



Certifier Assigning Rule

Create rule to assign requests to appropriate technicians. Learn more...

* Rule Name:

Description:

Business Workflow: 123

Requester > 1 Reviewer > 1 Approver > Executor

Notification : Disabled
No Templates Selected

ManageEngine
ADManager Plus

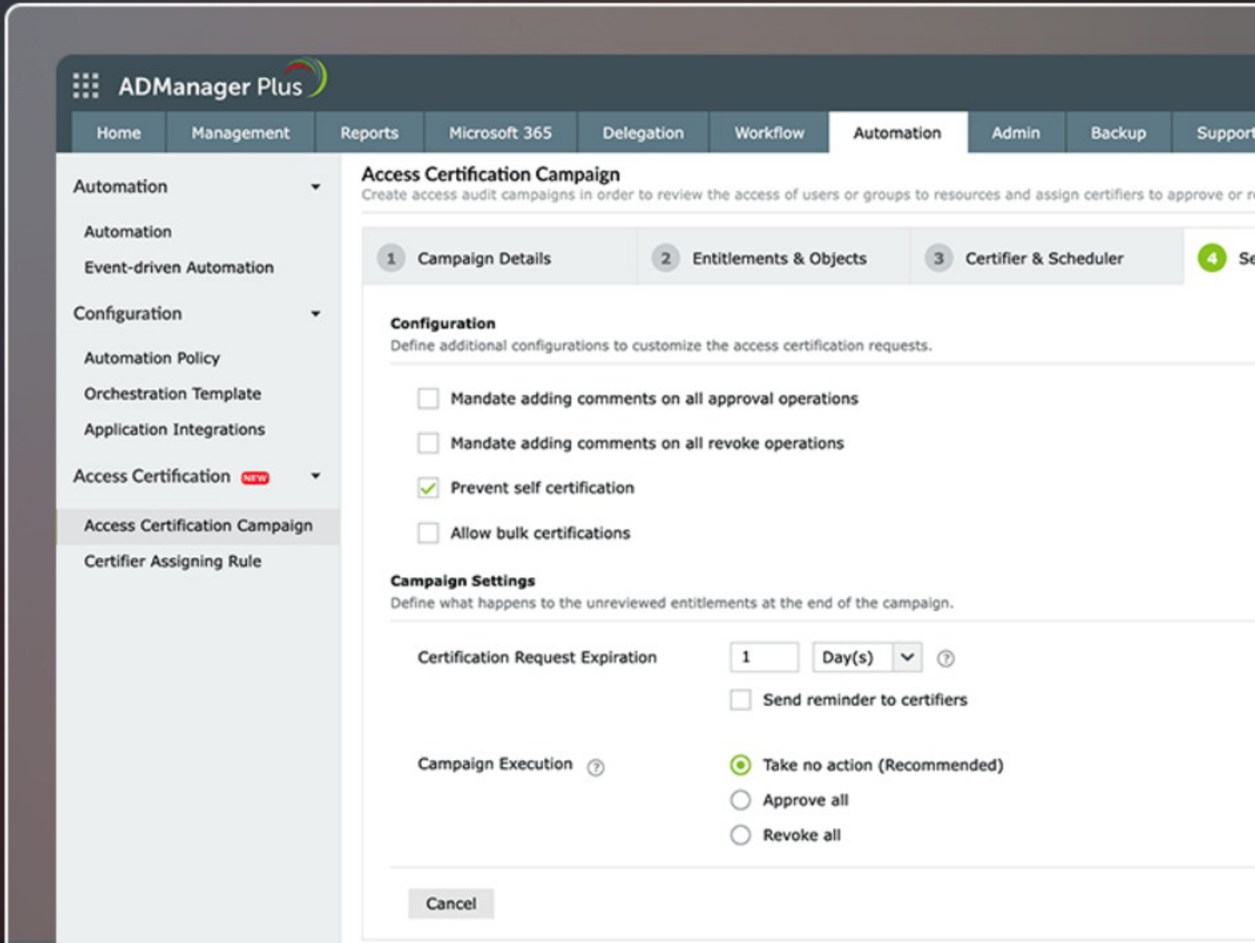
Customize your campaign

Configuration

Customize the access certification process by mandating comments for approval and revoke operations, preventing self-certification, and enabling bulk certifications for efficient management of access permissions

Campaign settings

Configure actions for certification requests that have not been reviewed upon campaign completion, including setting request expiration time, sending reminders to certifiers. Define default actions for approved or unapproved requests, such as taking no action, approving all, or revoking all



Access Certification Campaign

Create access audit campaigns in order to review the access of users or groups to resources and assign certifiers to approve or r

Configuration

Define additional configurations to customize the access certification requests.

- □ Mandate adding comments on all approval operations
- □ Mandate adding comments on all revoke operations
- ☑ Prevent self certification
- □ Allow bulk certifications

Campaign Settings

Define what happens to the unreviewed entitlements at the end of the campaign.

Certification Request Expiration: 1 Day(s)

□ Send reminder to certifiers

Campaign Execution:
- ● Take no action (Recommended)
- ○ Approve all
- ○ Revoke all

Compliance

HIPAA

Section/Article	Description
45 CFR 164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information
45 CFR 164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate
45 CFR 164.308(a)(4)(ii)(C)	Implement policies and procedures that establish, document, review, and modify a user's right of access to workstations, transactions, programs, or processes

PCI DSS v4.0 | SOX

Section/Article	Description
Requirement 7.2.3	Required privileges are approved by authorized personnel
Requirement 7.2.4	All user accounts and related access privileges are reviewed at least once every six months to ensure accounts and access remain appropriate based on job function
Requirement 7.2.5.1	All access by application and system accounts is reviewed periodically based on targeted risk analysis frequency
Section 302(a)(4)(A)	Signing officers are responsible for establishing and maintaining internal controls
Section 404	Management assessment of internal controls over financial reporting

ISO 27001:2022

Section/Article	Description
Control 5.15	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements
Control 5.18	Access rights to information and other associated assets shall be provisioned, reviewed, modified, and removed in accordance with established policies
Control 8.3	Access to information and other associated assets shall be restricted in accordance with established access control policies

GDPR

Section/Article	Description
Article 32(1)(b)	Implement appropriate technical and organizational measures to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems
Article 25	Data protection by design and by default: Implement appropriate technical and organizational measures to ensure data protection principles are integrated into processing

NIST CSF 2.0 | NIST SP 800-53

Section/Article	Description
PR.AC-1	Identity and access management processes and procedures are established and implemented
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
AC-2	Account Management: An organization manages system accounts, including establishing conditions for group membership, identifying authorized users, and reviewing accounts

COBIT 2019 | FISMA

Section/Article	Description
APO13.01	Establish and maintain an information security management system
DSS05.04	Manage identity and access rights: Ensure appropriate access to systems and data through proper identity and access management
Control AC-2	**Account management:** An organization manages information system accounts, including authorizing access and reviewing accounts
Control AC-6	**Least privilege:** An organization employs the principle of least privilege, allowing only authorized access necessary to accomplish assigned tasks

NERP CIP | FFIEC | COSO

Section/Article	Description
CIP-004-6 R4	**Personnel access authorization:** Verify that individuals have authorization for access to designated storage locations of BES Cyber System Information
CIP-004-6 R5	**Personnel access authorization:** Review access permissions to physical and electronic access rights to applicable systems at least once every 15 months
Information Security Booklet	**Access rights administration:** Financial institutions should implement processes to grant, review, and revoke user access rights
Internal Control Framework	**Control Activities:** Policies and procedures that help ensure management directives are carried out

ManageEngine
ADManager Plus

How Access Certification Campaigns address compliance standards

Systematic access governance and validation

Periodic validation of user access rights:

- ✓ Employees maintain only permissions necessary for current job functions
- ✓ Documentation and oversight required by auditors and regulatory bodies
- ✓ Comprehensive audit trails for compliance assessments

Authorized personnel validation:

- ✓ Designated approvers and reviewers validate access appropriateness
- ✓ Required privileges approved by authorized personnel (PCI DSS, HIPAA)
- ✓ Supports principle of least privilege (NIST CSF, FISMA, ISO 27001)

Compliance-mandated review frequencies:

- ✓ PCI DSS: Six-month cycles | NERC CIP: 15-month requirements
- ✓ Flexible scheduling configured to meet specific regulatory timelines
- ✓ Risk-based scheduling aligned with targeted risk analysis requirements

Management oversight and documentation:

- ✓ Executive approval workflows for access decisions
- ✓ Comprehensive audit-ready reporting across multiple frameworks
- ✓ Reduced compliance burden through automated processes

ManageEngine
ADManager Plus

Industry-specific compliance benefits

Tailored support across sectors

Healthcare organizations (HIPAA):

- ✓ Continuous validation of workforce access to electronic protected health information
- ✓ Appropriately restricted access to sensitive patient data
- ✓ Documentation of access decisions supporting HIPAA Security Rule compliance

Critical infrastructure (NERC CIP):

- ✓ Verified access authorization processes for BES Cyber System Information
- ✓ Mandated 15-month review cycles for personnel accessing sensitive energy systems
- ✓ Compliance documentation for regulatory assessments

Financial institutions (SOX, FFIEC, PCI DSS):

- ✓ Structured access rights administration meeting FFIEC guidelines
- ✓ Documented approval workflows supporting SOX internal control requirements
- ✓ Six-month review cycles for PCI DSS compliance with management oversight

Federal agencies (FISMA, NIST):

- ✓ Account management and authorization processes per NIST SP 800-53
- ✓ Least privilege enforcement aligned with FISMA requirements
- ✓ Security control implementation supporting federal compliance mandates

ManageEngine
ADManager Plus

Benefits of ADManager Plus' Access Certification Campaign

Compliance readiness

Adhere to regulatory requirements and organizational policies by maintaining a verifiable record of access reviews and modifications

Elevated security

Mitigate the potential for unauthorized access by identifying and revoking users' unnecessary access rights

Prevent privilege creep

Review access permissions regularly to prevent the accumulation of privileges, leading to a more efficient and manageable access control system

Mitigated insider threats

Regularly review users' access rights to identify and revoke unnecessary privileges, thus deterring malicious insider activities

Efficient resource management

By reviewing and revoking users' access to enterprise resources and group memberships, organizations can effectively lower license and subscription expenses

Improved efficiency

Streamline access management processes by running automated campaigns to identify and revoke access for over-privileged accounts

ManageEngine
ADManager Plus

Why ADManagerPlus?

ADManager Plus: Your go-to IGA tool

- Streamlined identity life cycle management
- 200+ pre-packaged reports
- Template-based, event-driven automations
- Periodic access certification campaigns
- Multi-level business workflows
- Secure data backups and recovery
- Integration with popular SIEM, HCM, ITSM and help desk tools
- iOS and Android mobile apps for on-the-go management

Explore ADManager Plus' full potential! Sign up now for a free product demo to explore additional features and functionalities

Register here

ManageEngine
ADManager Plus

GOT QUESTIONS?

Reach out to us

✉ support@admanagerplus.com

🌐 manageengine.com/products/ad-manager/