

Time Based Policy using IAM Service

In AWS IAM you can make a time-based policy using policy conditions, so that after the time expires the policy remains attached but becomes inaccessible (inactive).

Steps :

Step 1. Sign in to the AWS Management Console with an account that can create IAM policies.

The screenshot shows the AWS Management Console with the IAM service selected in the navigation bar. The left sidebar lists recently visited services: EC2, IAM, S3, Simple Notification Service, and AWS Health Dashboard. The main content area displays the 'Applications' section, which is currently empty. It includes a 'Create application' button and a note: 'No applications. Get started by creating an application.' Below this is another 'Create application' button.

Step 2. Go into IAM Service , In the left menu click Policies.

The screenshot shows the 'Policies' page under the IAM service. The left sidebar shows the 'Access management' section with 'Policies' selected. The main content area displays a table of existing policies, including 'AccessAnalyzerServiceRole', 'AdministratorAccess', 'AdministratorAccess...', 'AdministratorAccess...', 'AIOpsAssistantIncident...', 'AIOpsAssistantPolicy...', and 'AIOpsConsoleAdministrator...'. The table has columns for 'Policy name', 'Type', 'Used as', and 'Description'. A 'Create policy' button is visible at the top right.

Step 3. Click Create policy, Choose Visual editor tab, Select service Ex. S3 and Select the Actions you want to allow (ex. List,read,etc).

The screenshot shows the 'Create policy' wizard, Step 1: 'Specify permissions'. The left sidebar shows 'Step 1: Specify permissions' selected. The main content area is titled 'Specify permissions' and contains a 'Policy editor' section. It shows a list of actions for the S3 service, with 78 actions listed under 'Allow'. The 'Actions allowed' section allows filtering by action type. The 'Effect' dropdown is set to 'Allow'. Buttons for 'Visual', 'JSON', and 'Actions' are at the top right. At the bottom, there are links for 'Review and create' and 'Add actions'.

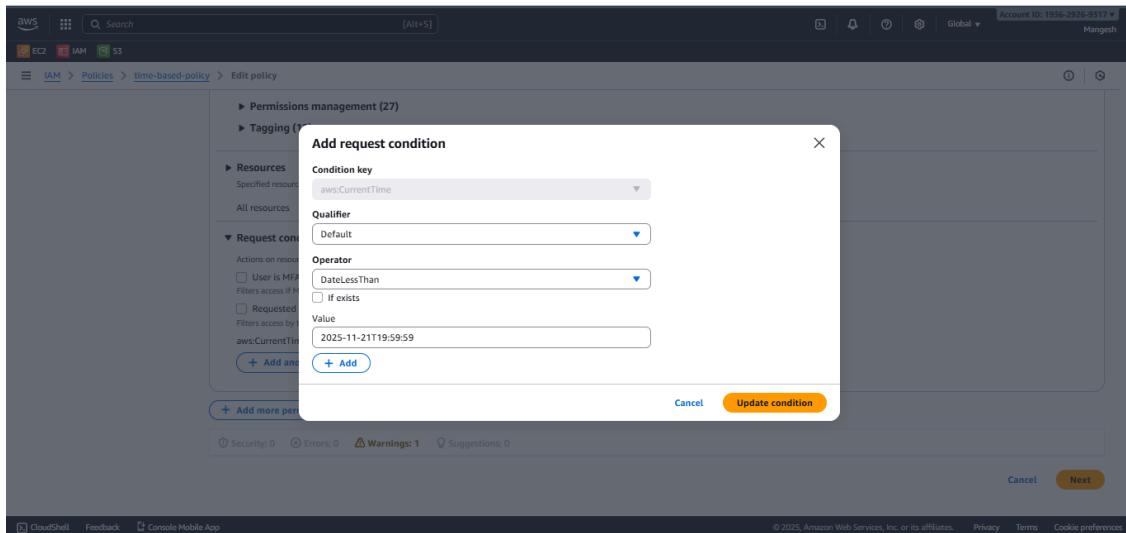
Step 4. Select the resources (All resources or specific buckets). → Scroll down to Request conditions → add condition

Condition key category → Date Operators

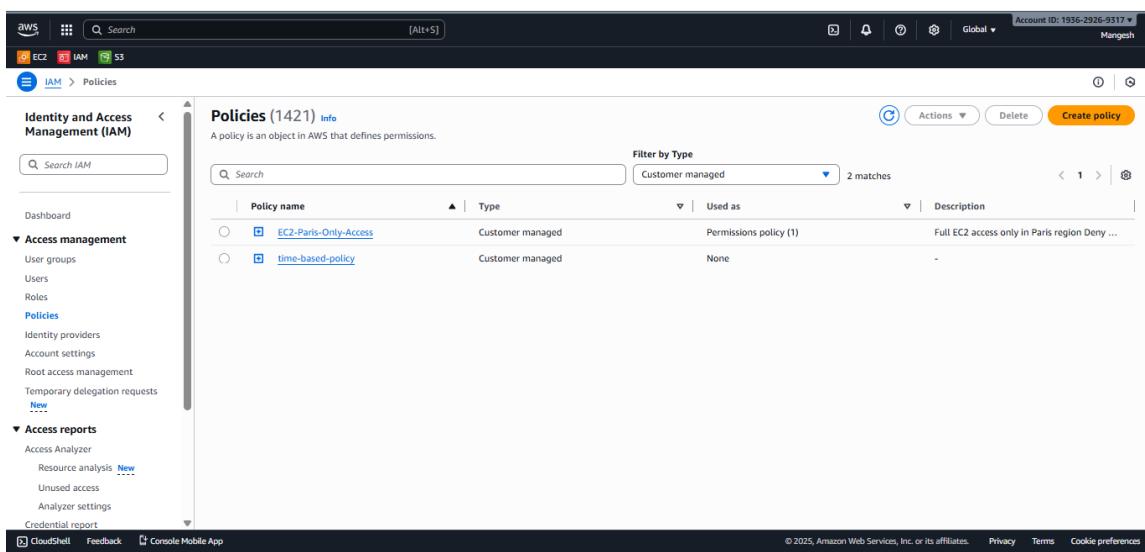
Condition key → aws:CurrentTime

Enter date and time in UTC format.

Add condition and click next.



Step 5 . Review and Create policy.



Policy created ' time-based-policy'

Step 6. Go to IAM → Users → home-02 → Add Permissions

Add permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options	
<input type="radio"/> Add user to group	Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
<input type="radio"/> Copy permissions	Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.
<input checked="" type="radio"/> Attach policies directly	Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1421)

Filter by Type	
<input type="text"/> Search	Customer managed
<input type="checkbox"/> Policy name ↗	Type
<input checked="" type="checkbox"/> EC2-Paris-Only-Access	Customer managed
<input checked="" type="checkbox"/> time-based-policy	Customer managed
Attached entities	
< 1 >	

[Cancel](#) [Next](#)

Step 7 . Add Permissions → Attach Policies directly → Select your policy name → Tik the checkbox → Click Add Permissions.

Add permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options	
<input type="radio"/> Add user to group	Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
<input type="radio"/> Copy permissions	Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.
<input checked="" type="radio"/> Attach policies directly	Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1421)

Filter by Type	
<input type="text"/> Search	Customer managed
<input checked="" type="checkbox"/> Policy name ↗	Type
<input checked="" type="checkbox"/> EC2-Paris-Only-Access	Customer managed
<input checked="" type="checkbox"/> time-based-policy	Customer managed
Attached entities	
< 1 >	

[Cancel](#) [Next](#)

Step 8. Review the policy that we attached.

home-02

Summary

ARN: arn:aws:iam::193629269317:user/home-02
Console access: Enabled without MFA
Created: November 21, 2025, 12:31 (UTC+05:30)
Last console sign-in: Today
Access key 1: Create access key

Permissions

Permissions policies (1)	
Permissions are defined by policies attached to the user directly or through groups.	
Filter by Type	
<input type="checkbox"/> Policy name ↗	Type
<input checked="" type="checkbox"/> time-based-policy	Customer managed
Attached via ↗	
< 1 >	

Permissions boundary (not set)

Policy has been attached to IAM user (home-02).

Step 9. Try to Access S3 bucket and create a S3 bucket .

IAM user read and list the S3 bucket.IAM user have an access to read and list the bucket .

IAM have access this bucket within the time 19:33:55 . → Action will succeed.

But IAM user cannot have an access to upload the data in the bucket because it has only read and list access.

Step 10. Check after the time limit of access is expired. → Access Denied.