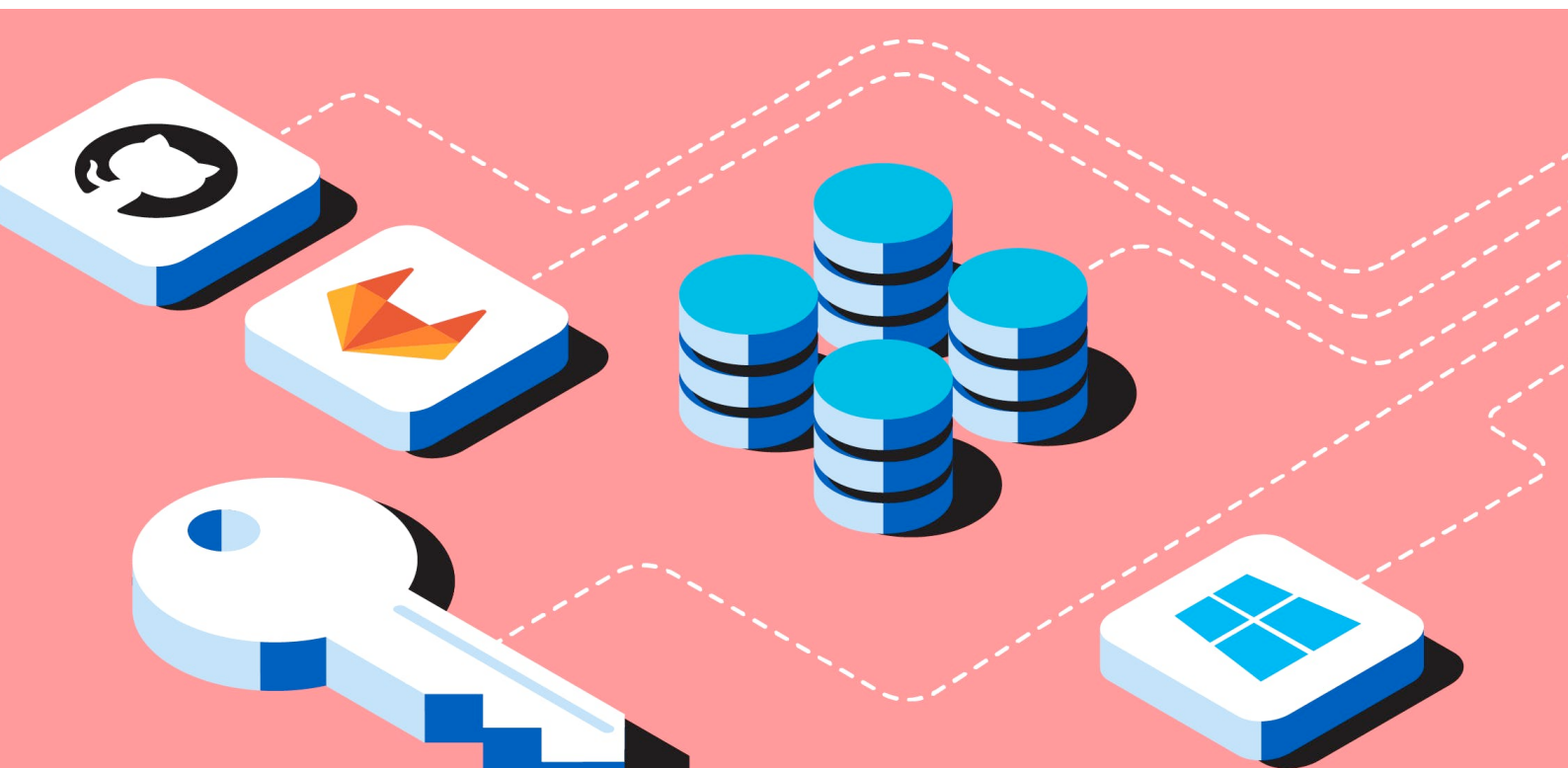


# Policy based Authentication

## SOLUTION BRIEF



## Policy based Authentication

---

### What is policy-based authentication?

AuthNull provides policy-based access for active directory and local privileged accounts.

What is a policy and why is it required?

- A policy provides granular access rules to resources, for example:
- An active directory user can access a single endpoint (instead of all the endpoints in the domain and ou)
- A active directory user can access an endpoint for one time only

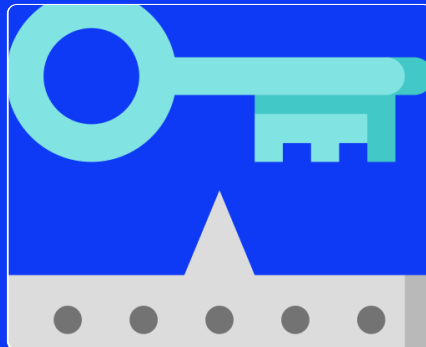
- A active directory user can access a specific endpoint user within a machine for a limited period
- A user can access all endpoints in the ou for the duration of his contract for example a month.

## What does AuthNull do?



### Discover's policies

AuthNull automatically discovers policies for active directory and local machines.



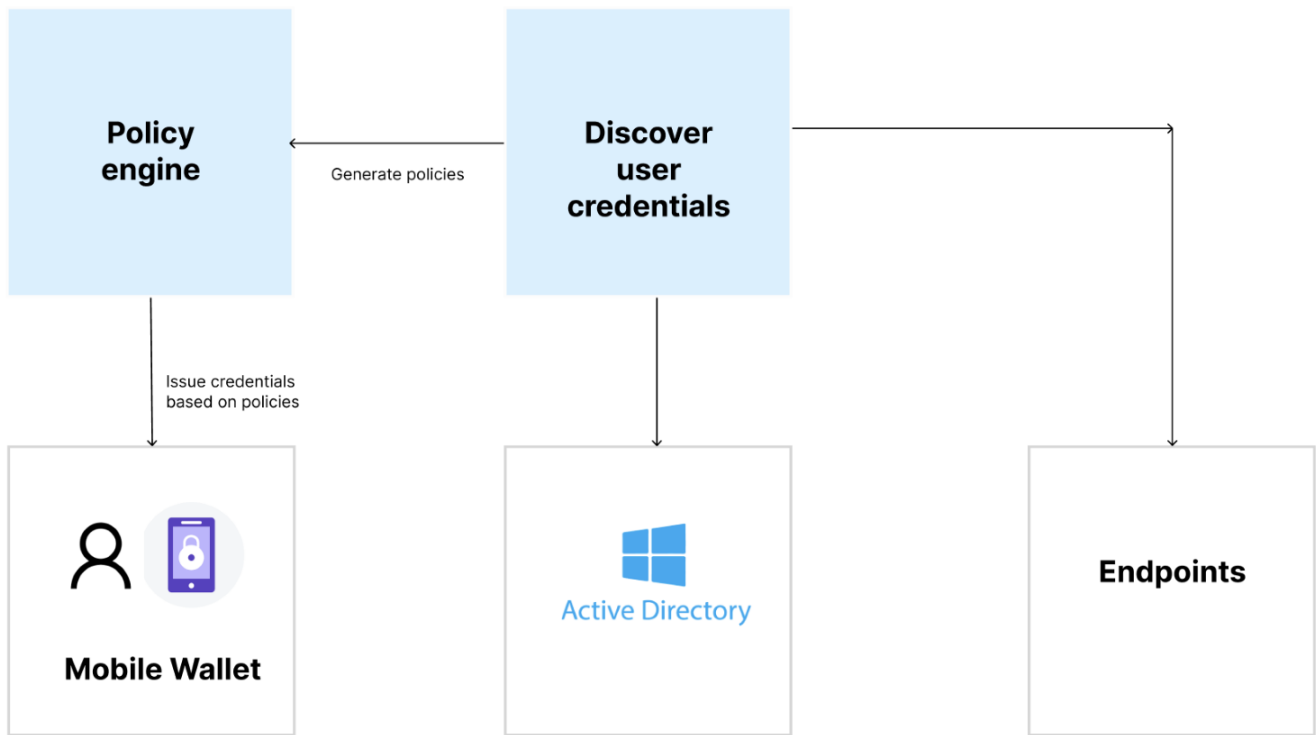
### Issues credentials

AuthNull automatically issues credentials for all users based on policies discovered



### Enables MFA

AuthNull quickly and seamlessly enables biometric MFA



## How does this work?

AuthNull's policy engine starts working as soon as you setup the endpoints and setup the tenant in "Audit mode" so that the system can then start discovering policies.

Administrators can then review requests on the **Authentication policies > Requests**

Authnull

Tenant has policies in audit mode

Dashboard
Endpoint
Jump Server
Credential Rotation
Authentication Policies
Requests
Policies
Authentication Logs
Service Account

### Requests

Access Type: Active Directory
Ou: Search OU
Domain: Search Domain
Endpoint: Search Endpoint

Applied Filters: logType: AD

Wallet User	Directory User	Destination Hostname	Destination IP	Policy Action	Auth Count	Policy Search	Action
[+] asif@kloudone.com	fox	windows-20-test	172.203.210.137		3	3 related policies found	:
[+] —	ali	windows-test-17	57.151.91.59		2	3 related policies found	:
[+] asif@kloudone.com	fox	windows-test-17	57.151.91.59		13	3 related policies found	:
[+] —	asif@kloudone.com	windows-test-17	57.151.91.59		17	3 related policies found	:
[+] hussain@authnull.com	fox	4.227.155.162	—	Approved	18	3 related policies found	:

1-100 of 100

On the create policy screen, administrators can select default options to create a policy:

Creating new policy for fox

What ?

Directory Users

fox

Endpoints and Endpoint Groups

Endpoints

Endpoints List

windows-20-test

Who ?

Wallet Users

asif@kloudone.com

Policy Action

Allow

In Review

Activate

Once policies are active administrators can see authentication logs:

Authnull

Dashboard

Endpoint

Jump Server

Credential Rotation

Authentication Policies

Requests

Policies

Authentication Logs

Service Account

Authentication Logs

Username

Log Type

Endpoint

Search username

Search Access Type

Search Endpoint

Wallet User	Endpoint User	Destination	Destination	Log Type	Protocol	OS	Ou	Domain
asif@kloudone.com	fox	windows222	20.55.70.100	Active Directory	RDP	windows	ou=rider-park	dc=Authnull,dc=co
asif@kloudone.com	windows222admi	windows222	20.55.70.100	Service Account	SSH	windows	ou=rider-park	dc=Authnull,dc=co
asif@kloudone.com	fox	windows222	20.55.70.100	Active Directory	RDP	windows	ou=rider-park	dc=Authnull,dc=co
asif@kloudone.com	fox	windows222	20.55.70.100	Active Directory	RDP	windows	ou=rider-park	dc=Authnull,dc=co
asif@kloudone.com	fox	windows222	20.55.70.100	Active Directory	RDP	windows	ou=rider-park	dc=Authnull,dc=co
asif@kloudone.com	fox	windows20-2test	4.227.158.182	Active Directory	RDP	windows	ou=rider-park	dc=Authnull,dc=co
asif@kloudone.com	fox	windows20-2test	4.227.158.182	Active Directory	RDP	windows	ou=rider-park	dc=Authnull,dc=co
asif@kloudone.com	fox	windows20-2test	4.227.158.182	Active Directory	RDP	windows	ou=rider-park	dc=Authnull,dc=co
asif@kloudone.com	fox	windows-test-17	57.151.91.59	Active Directory	RDP	windows	ou=rider-park	dc=Authnull,dc=co
asif@kloudone.com	fox	windows-test-17	57.151.91.59	Active Directory	RDP	windows	ou=rider-park	dc=Authnull,dc=co
asif@kloudone.com	windowsadmin2	windows-test-18	4.227.155.87	Service Account	SSH	windows	ou=rider-park	dc=Authnull,dc=co

"AuthNull's policy discovery helps reduce our workload. We simply love it.."

## The path to zero trust

AuthNull's Policy Engine enables a significant step towards achieving Zero Trust in privileged access without needless friction. By automating the discovery of authentication policies, AuthNull streamlines the process and bolsters security without introducing friction and delays both in the secops, and in the user experience.

Here's the set of steps required to get to zero trust with AuthNull

Milestone	How?	Steps	
Onboard users	Install AD Agents	<input checked="" type="checkbox"/>	Install AD agent
		<input type="checkbox"/>	Issue wallet invites
		<input type="checkbox"/>	Users download apps
Onboard endpoints	Install Agents on endpoints	<input type="checkbox"/>	Configure agent
		<input type="checkbox"/>	Verify MFA
		<input type="checkbox"/>	Issue Credentials
Policy setup	Setup policies	<input type="checkbox"/>	Start in audit mode
		<input type="checkbox"/>	Discover policies
		<input type="checkbox"/>	Create policies
		<input type="checkbox"/>	Flip to enforcement

# Moving to Zero Trust

Tenant Config

Tenant Name

kloudlearn

> MFA device + MFA settings

> Application Control

> Credential store and sharing

> Authentication Policy

Authentication Policy

Audit - this will audit existing policies and create new policies (learn the system)

Audit - this will audit existing policies and create new policies (learn the system)

Policy - Simulate enforcement policies and see the impact of blocked policies

Live mode - Zero trust (block everything but trusted) - warning this requires policies to be available

Live mode - Zero trust (block everything but trusted) - warning this requires policies to be available

Moving to zero trust requires that the administrator change the global tenant settings to policy enforcement mode as shown above.

To access this setting go to **Tenant > Tenant Config > Authentication Policy** and change the value to **“Live mode”**

Once these set of steps are implemented, you’re infrastructure is ready and implementing Zero Trust.



## Contact Information

We would love to hear from you!

Asif Ali | [a@authnull.com](mailto:a@authnull.com) | 408-368-3404