Ø AuthNull

Active Directory Privileged Access SOLUTION BRIEF

Privileged Access for Active Directory

AuthNull provides simplified privileged access for Active directory

- Privileged Account Management for Active Directory user accounts
- Privileged Session Management and Recording
- Credential rotation for Active Directory users

- Automated on-boarding and off-boarding of users
- Creates policies for all permissions that the users have access to.

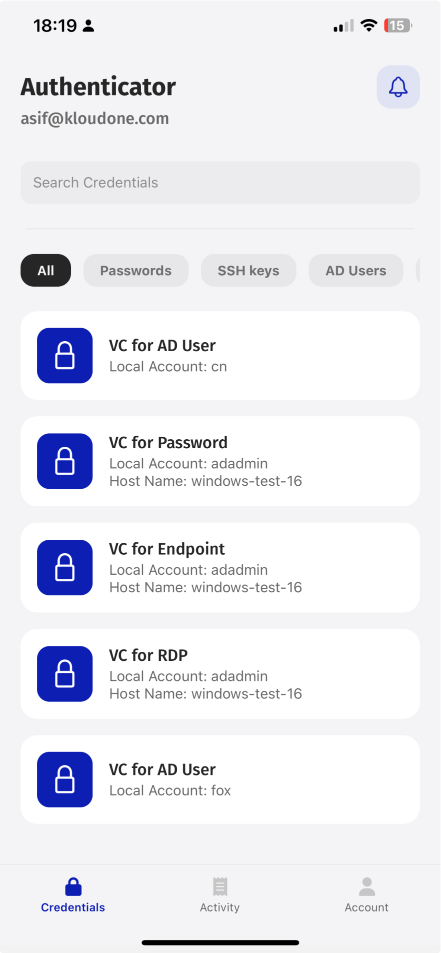
AuthNull enables active directory integration with the help of an Agent that sits near the Domain controller.

On-boarding and off-boarding of users

When user's are on-boarded to active directory (via a HR system), they are automatically on-boarded to AuthNull, and when they are removed from Active Directory - their wallets and credentials are automatically removed.

All users who are on-boarded to AuthNull receive Wallet invites. When the users register the wallet with their identity, they typically setup their biometric MFA.

With the wallet in place, users can receive credentials and authenticate to systems with biometric MFA.



Authenticator
asif@kloudone.com

VC for AD User
Local Account: cn

VC for Password
Local Account: adadmin
Host Name: windows-test-16

VC for Endpoint
Local Account: adadmin
Host Name: windows-test-16

VC for RDP
Local Account: adadmin
Host Name: windows-test-16

VC for AD User
Local Account: fox

Automated granular policy creation for Active Directory

AuthNull discovers granular controls based policies automatically

AuthNull discovers user policies based on existing active directory authentication and authentication logs. This enables:

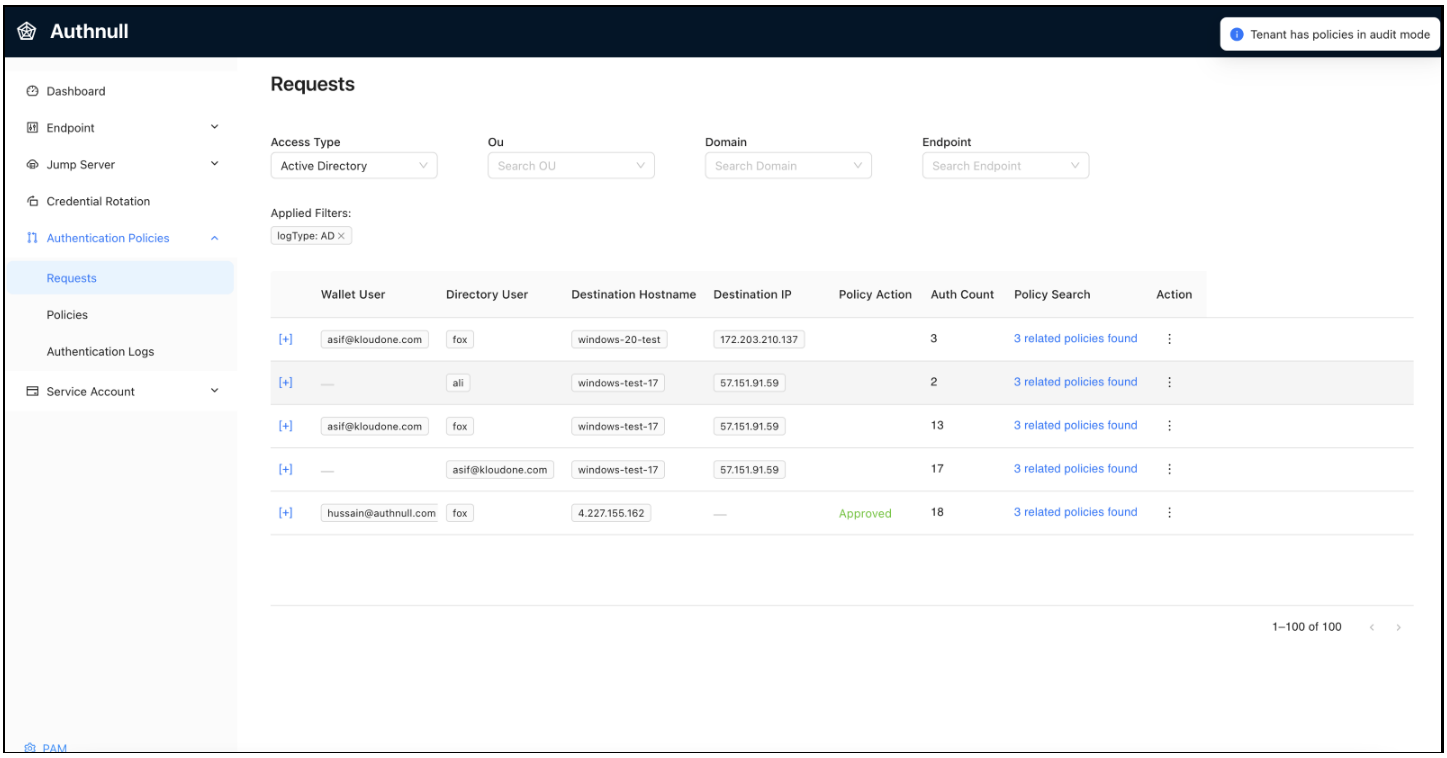
- Granular policy creation
- Discovery of credentials,
- Rotation of credentials based on tenant configuration
- Issues identities for all active directory users; removes users as they are removed from active directory.
- Creates policies for all permissions that the users have access to.

Granular Policy Creation & Credential Issuance

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**

These policies are discovered automatically for active directory accounts or local privileged accounts



Requests

Access Type: Active Directory

Ou: Search OU

Domain: Search Domain

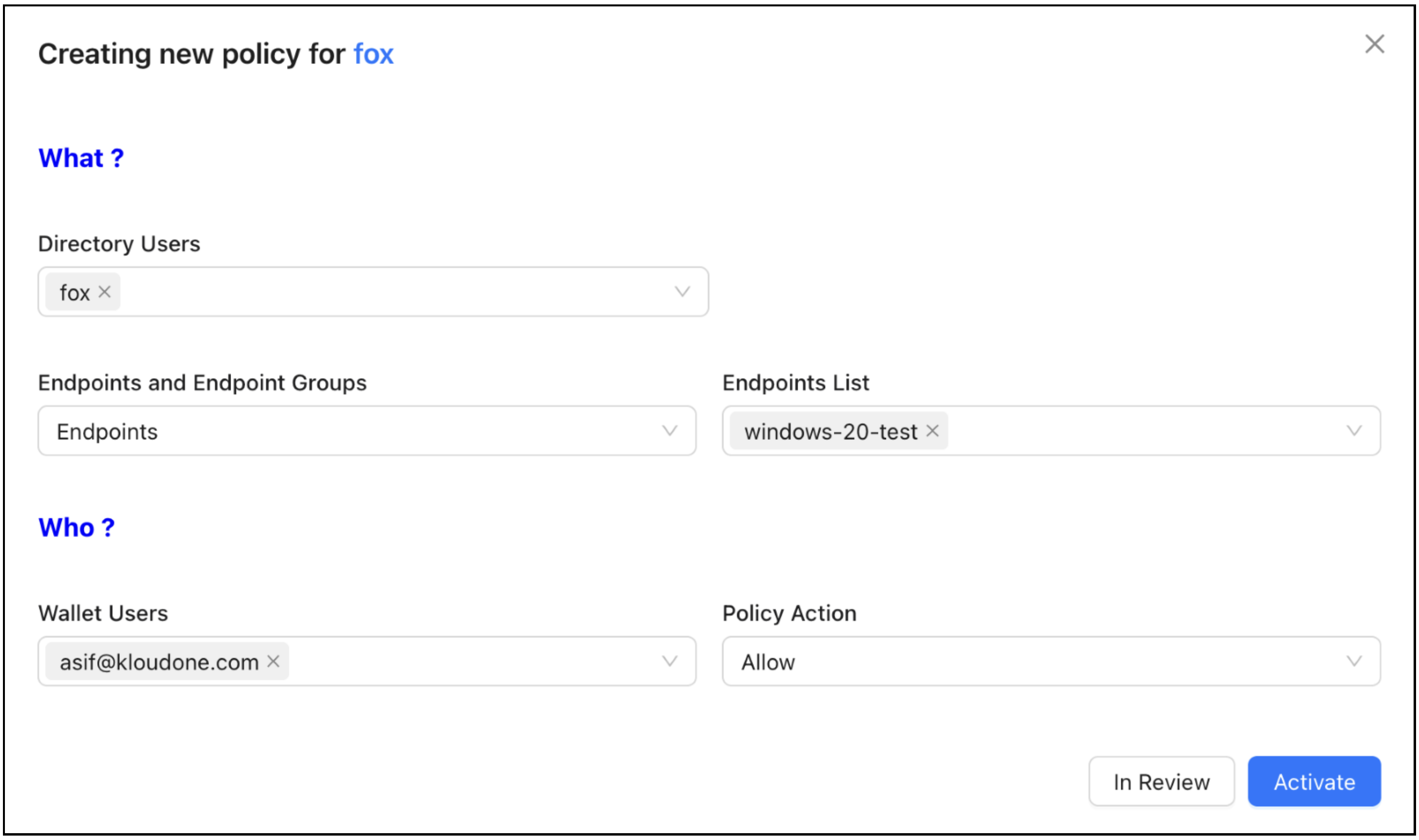
Endpoint: Search Endpoint

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 ?

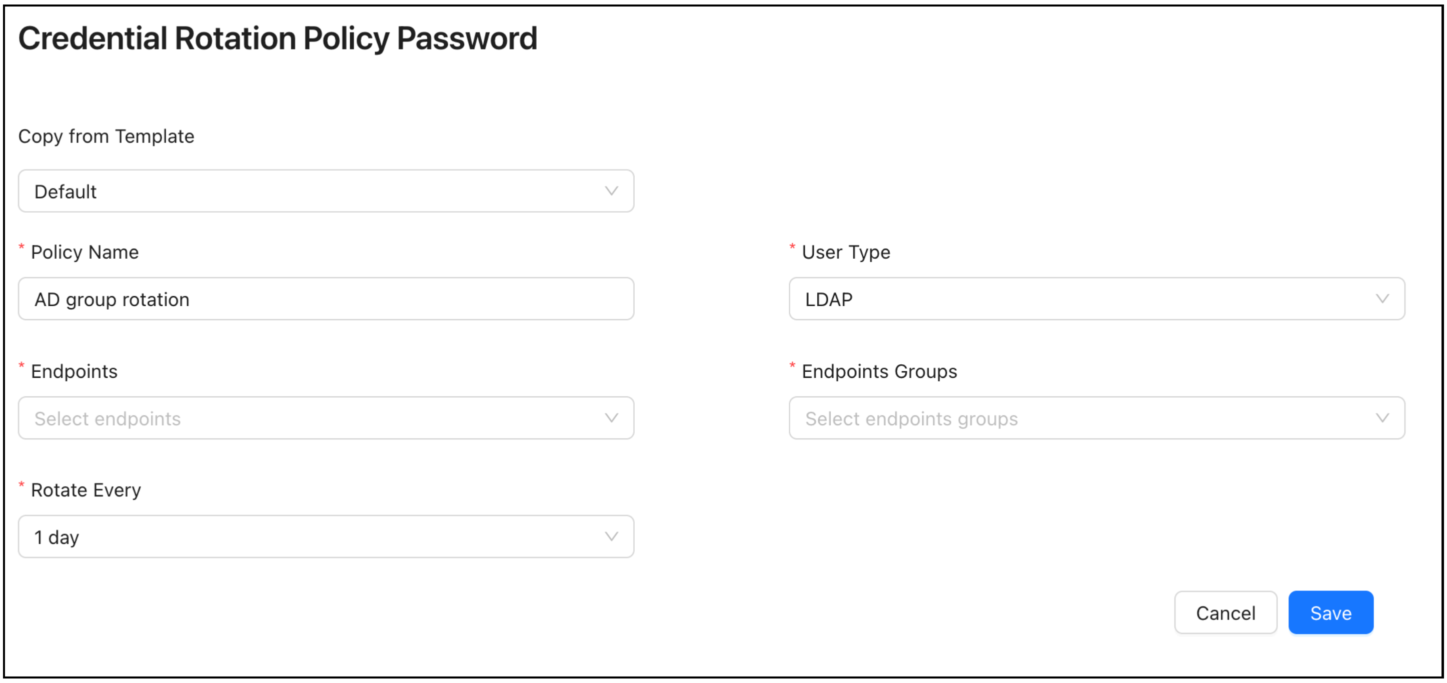
Wallet Users: asif@kloudone.com

Policy Action: Allow

When these policies are created, users are notified on their mobile wallets with a credential specific to the policy that is extremely granular.

Credential Rotation

Admins can quickly setup the Active directory credential rotation. policies and rotate credentials for all users. As credentials are rotated, the users receive them on their wallets.



Credential Rotation Policy Password

Copy from Template

Default

* Policy Name

AD group rotation

* User Type

LDAP

* Endpoints

Select endpoints

* Endpoints Groups

Select endpoints groups

* Rotate Every

1 day

Enabling access to new users

New users simply need to attempt to connect (using RDP) or a direct login to the target machine. When they do that, new authentication requests popup on the Authentication requests screen which can be converted to a policy instantaneously.

Remember that when this happens (a) new policies are created (b) new granular credentials are created and (b) possibly credentials are rotated (while using shared accounts).

> “Biometric MFA and Identity Protection is baked into AuthNull”

Biometric MFA & PKI

Biometric MFA that is AAL2 compliant is baked into AuthNull. When users are on-boarded, the wallet requires user verify the identity with a wallet key. This wallet key uses public key cryptography and uses a public / private key pair which each user receives. This private key is used to sign credentials received by the user, which are then verified by the user’s public key by the organization.

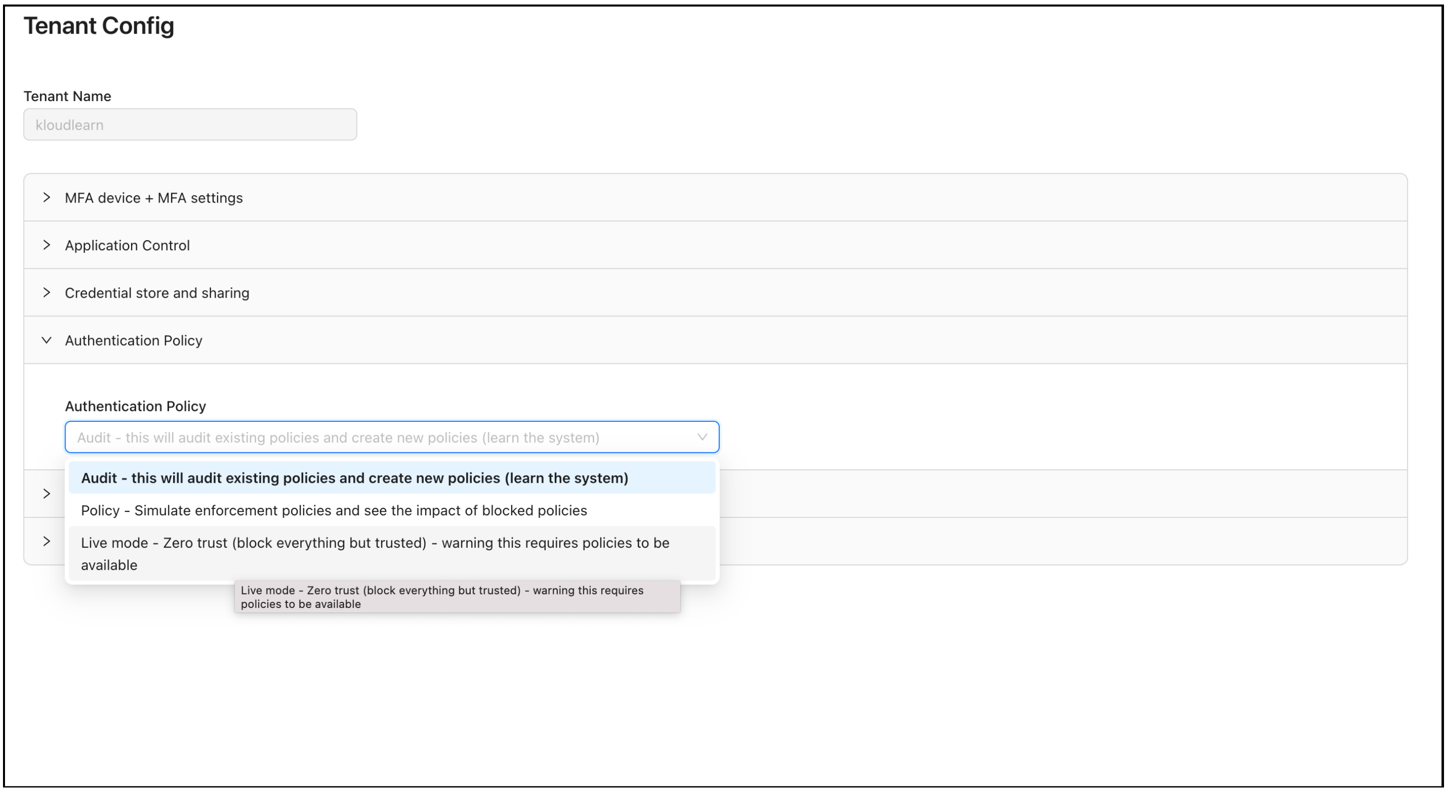
Two roots of trust: AuthNull relies on user’s public-private key pair as well as organization’s public private key pair in order to sign, create and verify credentials

Path to Zero Trust on Active Directory

To get to Zero trust on Active Directory here are the set of steps that need to be followed.

Milestone	How?	Steps	
Onboard active directory	Install AD Agents	□	**Install AD agent**
Onboard users	Send user wallet invites (automated process)	☑ □	**Issue wallet invites** **Users download apps**
Onboard endpoints	Install Agents on endpoints	□ ☑ □	**Configure agent** **Verify MFA** **Issue Credentials**
Policy setup	Setup policies	□ □ □ □	**Start in audit mode** **Discover policies** **Create policies** **Switch to Zero trust**

Moving to Zero Trust



Tenant Config

Tenant Name

kloudlearn

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 | 408-368-3404