Add Policy

https://campus.barracuda.com/doc/93201523/

The table below shows the app versions for which each policy is supported, by operating system.

Policy Name	Android	iOS	Linux	macOS	Windows
Block jailbroken devices	0.20.46540	0.20.46540	-	-	-
Detect disk encryption	0.22.0	0.22.0	-	0.22.0	0.24.0
Detect firewall enabled	-	-	-	0.23.0	0.24.0
Detect screen lock enabled	0.20.46540	0.11.10	-	-	-
Reauth supported	0.22.0	0.22.0	0.22.0	0.22.0	0.22.0
OS version outdated	0.23.0	0.23.0	-	0.23.0	0.23.0
Detect antivirus status	-	-	-	-	0.24.0

How Are Policies Implemented?

The CloudGen Access app runs in user space, and, as such, relies on system-supported APIs that implement non-kernel access to the attribute information. In particular, in the case of disk encryption, firewall, screen lock, and anti-virus policies, the CloudGen Access app relies on the following specific APIs:

- Windows Security Center (WSC) in the case of Windows apps – third-party firewall and anti-virus software must be compliant
- IOKit for iOS and macOS
- DevicePolicyManager for Android apps.

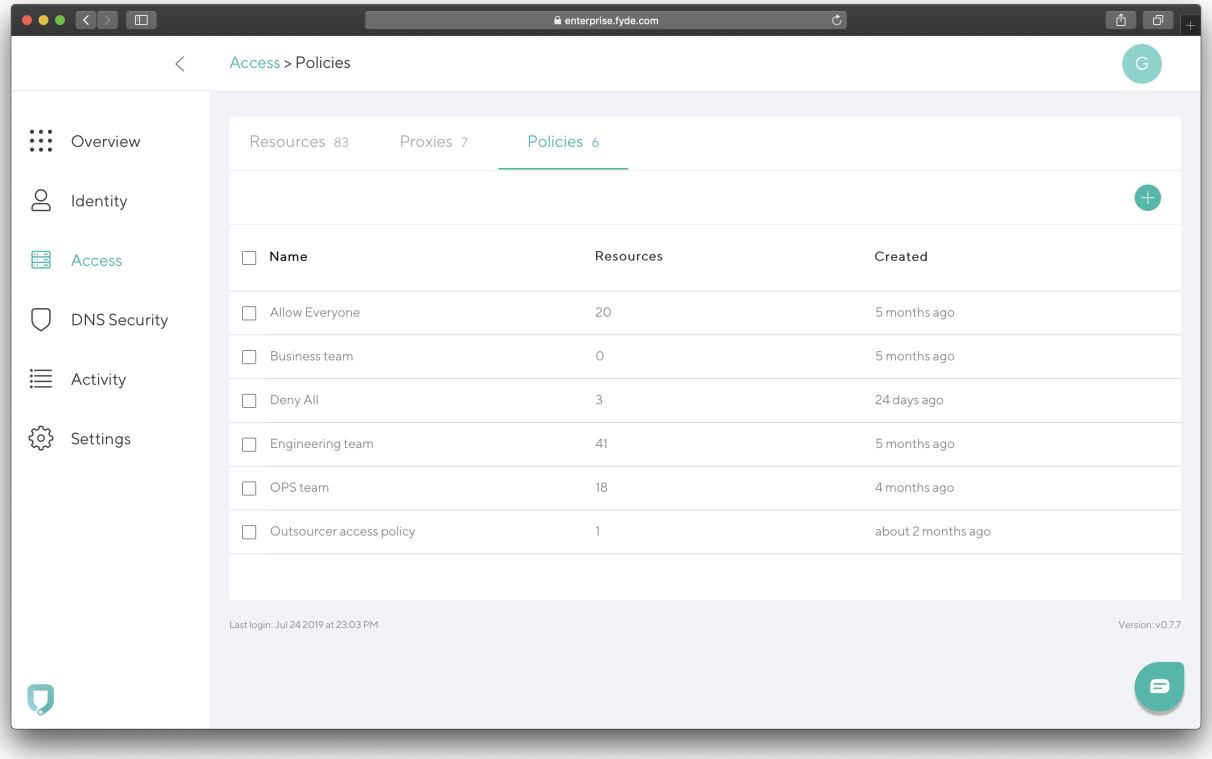
The RootBeer library for Android is used for detecting jailbroken devices. For iOS, rootkits are verified by checking for certain files and known apps, as well as whether the file system may be accessed outside of the app sandbox.

Finally, for detecting an outdated OS version, semantic versioning is compared with the version that the system administrator selects.

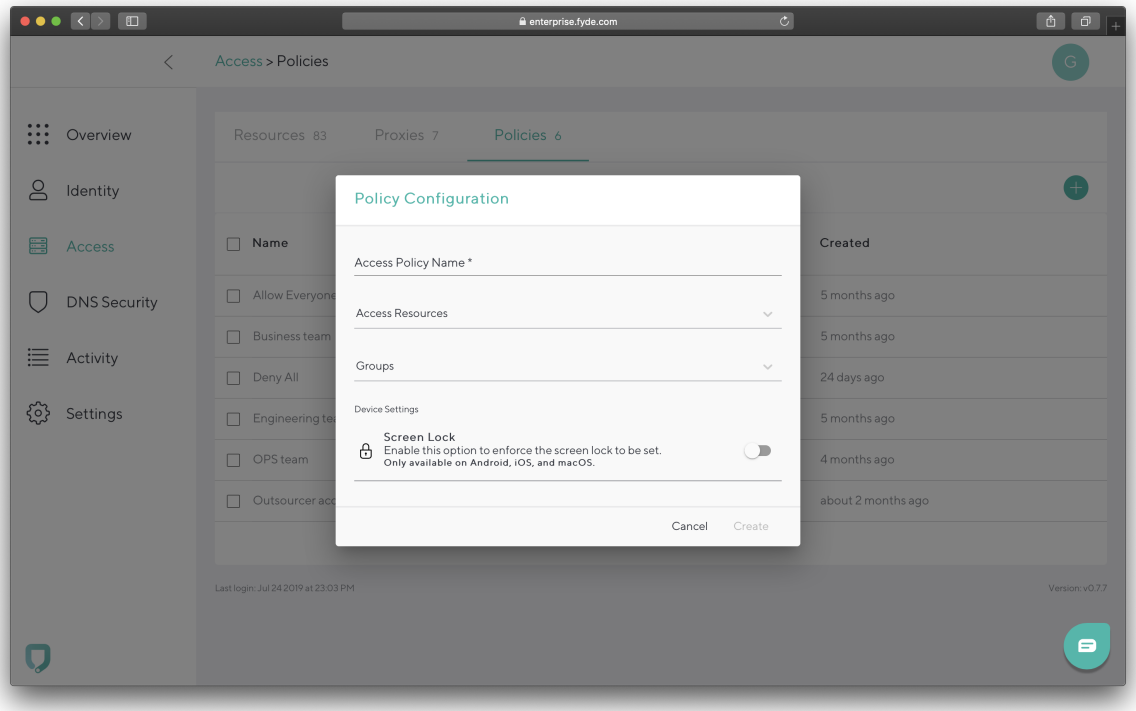
Adding a Policy

To add an access policy:

1. Go to **Access** and navigate to **Policies**. Click the **+** icon in the top right.



2. Add the following:
   - **Access Policy Name** – Name to identify the policy.
   - **Access Resources** – Resources associated with the policy.
   - **Groups** – Groups that will have access to the resources.
   - **Device Settings** (optional) – Configure rules that devices need to comply with to access the resources.



3. Click **Create**.

Figures

1. ec-access-add-policy.png
2. ec-access-policies.png