Silverfort

Silverfort's deny access policies

Silverfort can deny access requests for every type of user, service account, access method, and resource in real time, halting any unauthorized access

Silverfort's 'Deny Access' policy capabilities enable organizations to enforce access controls on all users, systems, and access methods. Using Silverfort's deny policies, admins can define specific rules and conditions for blocking access attempts based on various factors such as user identity, authentication protocol, device security posture, user location, time of access, and risky behavior.

Silverfort **automatically blocks access in real time** when an authentication attempt or access request violates the defined policy parameters. By proactively applying deny access policies, Silverfort users naturally reduce their identity attack surface and protect against future identity threats.

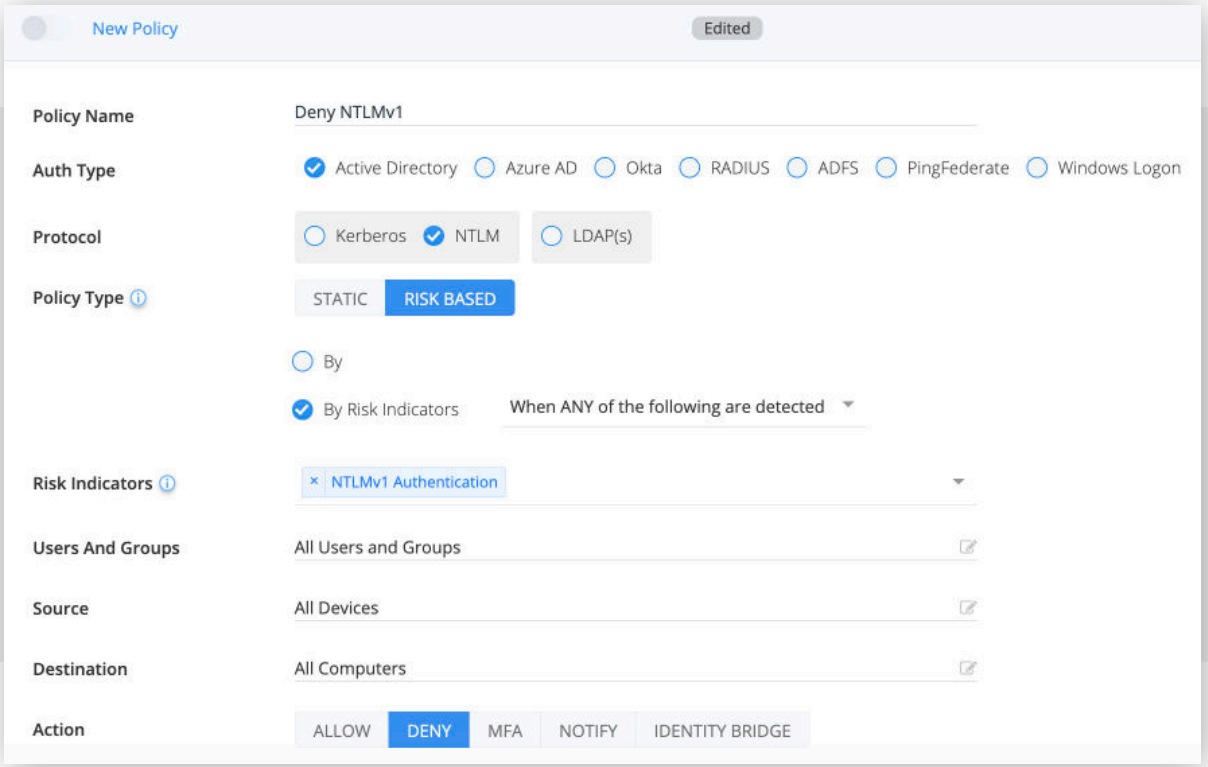
Silverfort's integration with all leading Identity Providers (IdP) enables it to enforce deny access policies on all resources on-prem and in the cloud, providing organizations with centralized control and visibility into all user and resource activity. Additionally, Silverfort enables admins to monitor access attempts, investigate security incidents, and ensure compliance with regulatory requirements.

How to create a deny access policy

Here are a few popular deny access use cases that many of our customers use within their Silverfort policy screen:

- **Block attacks**: Block specific types of attacks targeting users and resources. For example, block users from performing NTLMv1 authentication which can be easily cracked by attackers that intercept its authentication traffic. By blocking NTLMv1 traffic you effectively disarm attackers' ability to leverage protocol weaknesses for malicious access.
- **Identity segmentation**: Deny access based on the user access privileges and the device they are using. For instance, critical infrastructure can be protected to prevent unauthorized access, even if permissions were mistakenly granted.
- **Contain risk**: Only allow user access when certain conditions are met, such as using strong encryption from resource A to resource B. All other types of access are denied, containing potential risks.
- **PAM server enforcement**: Enforce strict access policies by allowing connectivity exclusively through designated PAM servers, denying all other connection attempts and ensuring centralized and secure privileged access control.
- **Deny specific locations**: Deny users from accessing applications or devices from specific locations.

How to create a deny access policy



A Silverfort policy to deny access via NTLMv1

In Silverfort's **Policies** screen, create a new policy. Check your IdP as the **Auth Type**, then check either **Kerberos/NTLM** or **LDAP**, depending on your needs. Choose **Risk Based** for the policy type and for User and Group, set the users or group of users you want to assign to this policy. Next, under **Action**, choose **Deny**.

Once enabled, this will automatically deny access to any account under this policy. If this account was compromised, this policy would deprive an adversary of the ability to use it for malicious access.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.