Silverfort

Silverfort Smart Policy for Service Accounts

Scale service account protection in bulk with behavior-based policies that never interfere with service operations

What is Smart Policy?

With Silverfort's Smart Policy, customers can automatically create policies for groups of service accounts without disrupting critical services. Once a group or an organizational units (OU) of service accounts is added to its scope, the Smart Policy will continuously look for accounts showing consistent activity over time and extend the right security policy to each. As the Smart Policy is dynamic, it will automatically detect new or removed service accounts from the selected groups in your Active Directory.

Smart Policy enables organizations with many service accounts to apply security policies in bulk, instead of performing the time and labor-intensive process of creating policies one-by-one, monitoring for policy deviations, and manually enforcing deny policies. This allows a greater focus on more complex and dynamic service accounts.

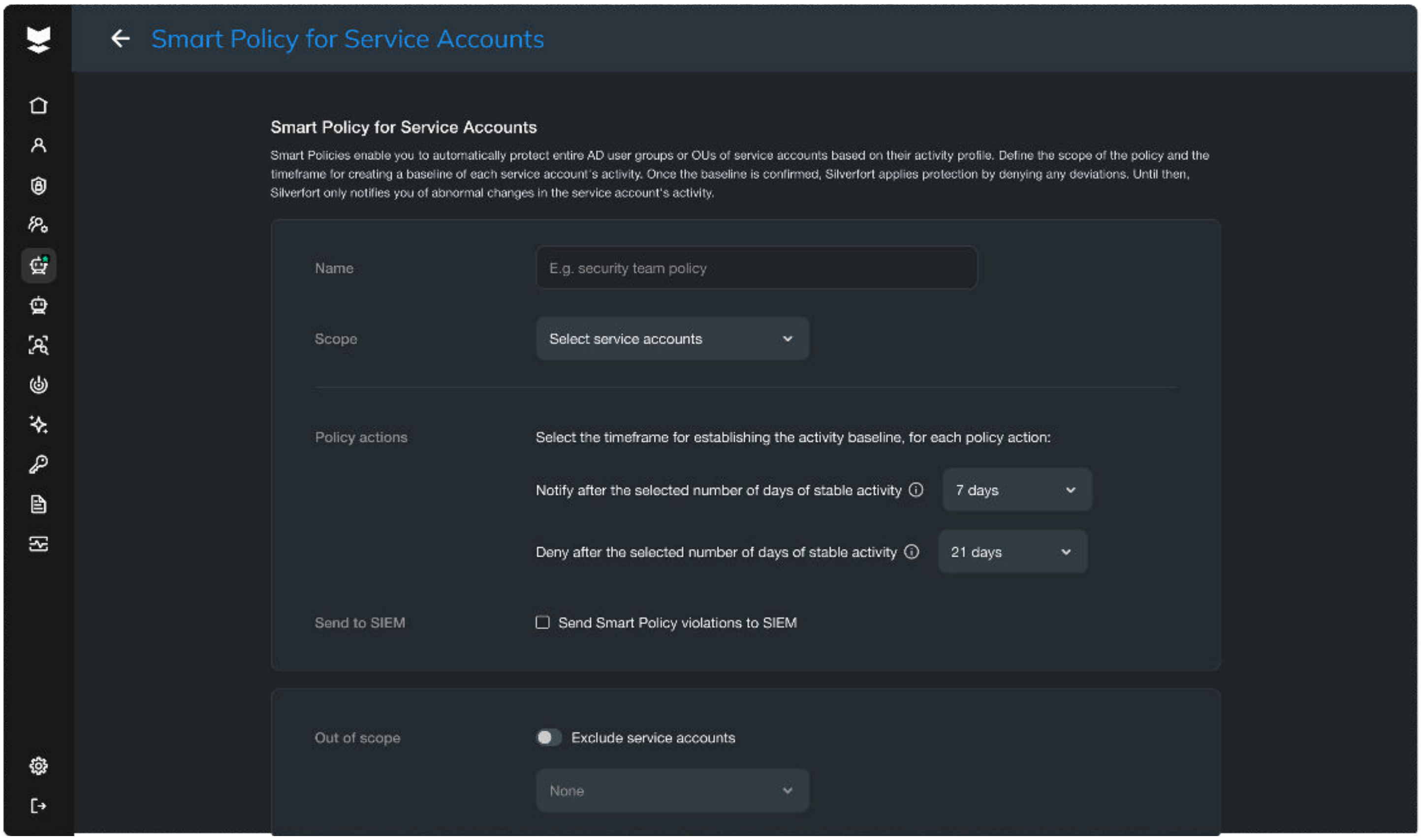
How does Smart Policy work

The Smart Policy runs in cycles, scanning service accounts for baseline changes, deciding on action, and modifying policies. For each service account in the Smart Policy scope:

1. Silverfort monitors the last time the account's sources, destinations, or protocols changed.

2. Once the service account reaches a desired period of consistent behavior, a policy can be automatically activated to notify you of any deviation.

3. If the account behavior remains consistent for a prescribed time, the policy will automatically change to deny any authentication that deviates from the confirmed baseline behavior



← Smart Policy for Service Accounts

Smart Policy for Service Accounts

Smart Policies enable you to automatically protect entire AD user groups or OUs of service accounts based on their activity profile. Define the scope of the policy and the timeframe for creating a baseline of each service account's activity. Once the baseline is confirmed, Silverfort applies protection by denying any deviations. Until then, Silverfort only notifies you of abnormal changes in the service account's activity.

Name: E.g. security team policy

Scope: Select service accounts

Policy actions: Select the timeframe for establishing the activity baseline, for each policy action:

Notify after the selected number of days of stable activity ⓘ 7 days

Deny after the selected number of days of stable activity ⓘ 21 days

Send to SIEM: □ Send Smart Policy violations to SIEM

Out of scope: ○ Exclude service accounts

None

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.