SILVERFORT

How Silverfort Secures Former Employee Accounts

Many organizations spend a lot of time onboarding new employees and making sure they have access to everything they need; however, the same care is often lacking when it comes to offboarding. When an ex-employee is not properly offboarded, their accounts pose a significant risk: external attackers are known to compromise unmonitored leaver accounts. The major identity security risks include:

- Account Takeover
- Malicious 3rd party access
- Lateral movement attacks
- Data breaches
- Compliance violations
- Operational disruption

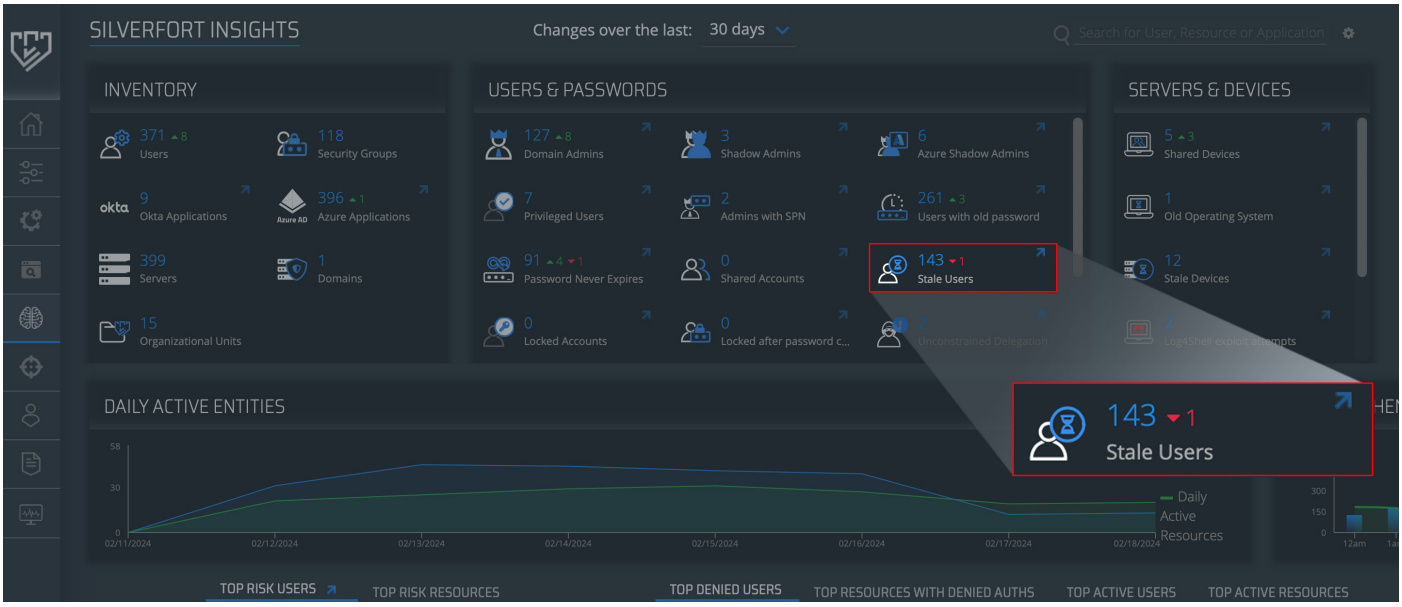
Complete Visibility and Protection to All Stale Users

Silverfort enables Identity teams to easily discover former employee accounts in their environments and either delete them or remove their permissions. Silverfort classifies accounts that have not been used for a year or more as “Stale Users”. With Silverfort you can gain complete and continuous visibility into stale users and apply appropriate security measures, such as enforcing block access policies to these user accounts.

Visibility Into Stale Users

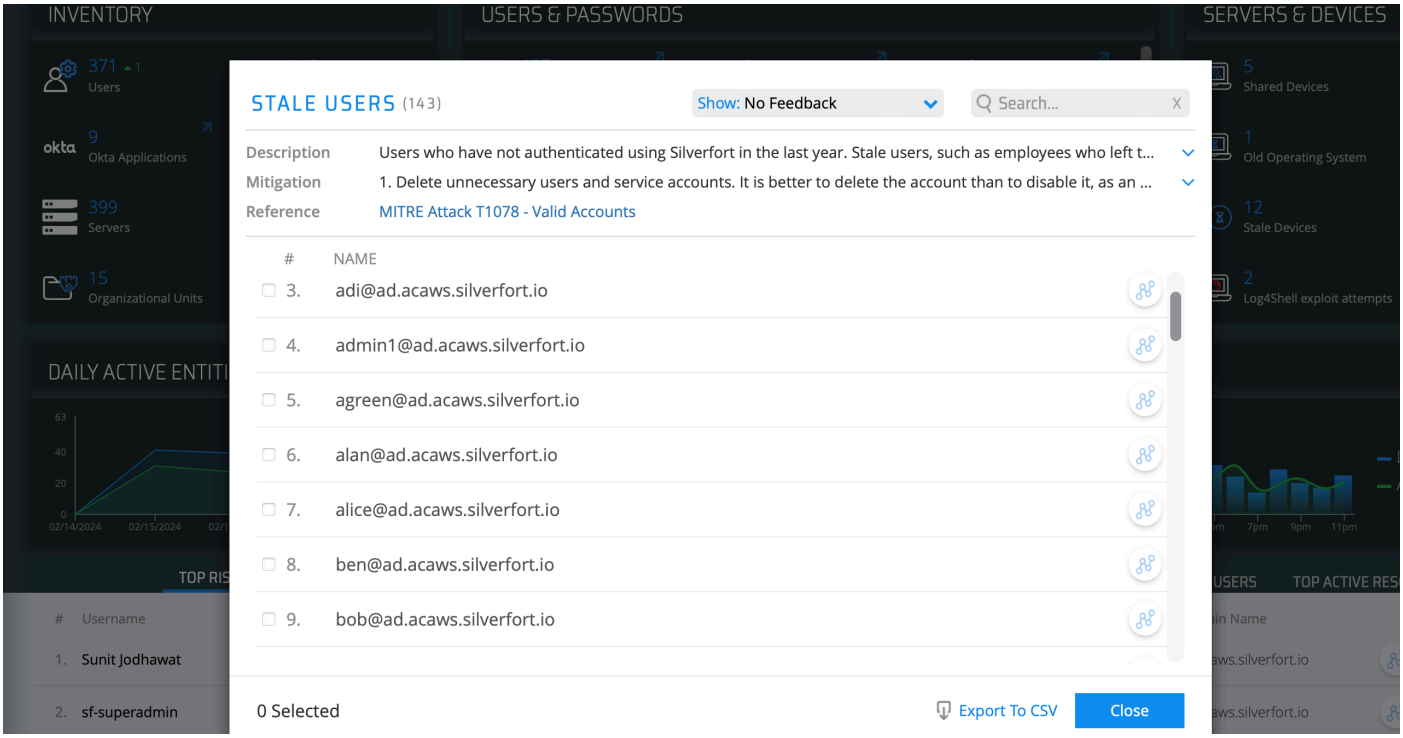
Silverfort automatically discovers all accounts in your environment, including stale user accounts, and provides real-time visibility into all user activity. This enables you to detect and respond to potential security threats — including blocking the access of any accounts that display anomalous behavior.

In Silverfort’s Insights screen, you will see an in-depth identity inventory that displays the types of users and resources in your environment as well as weaknesses in your security. Under **Users & Passwords**, you can find the entire list of stale users in your environment.



Screenshot #1: Discovering the number of stale users in the Insights screen

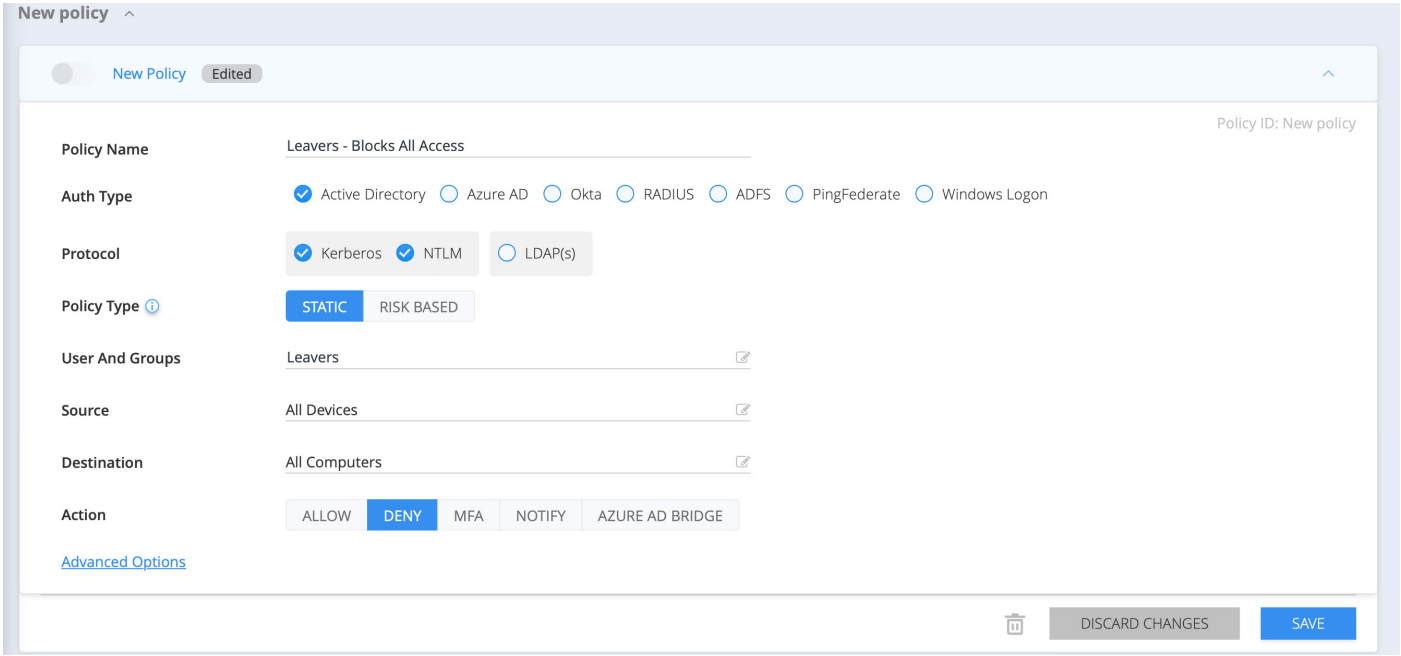
Clicking on the **Stale Users** space opens a window with full details on these accounts. Now that you have the names of these stale users, you can locate them in its identity provider (IdP) and either remove their permissions, delete them, or apply a deny access policy to the user account.



Screenshot #2: Displaying the complete list of stale users

Creating a Leaver Policy

To take a more proactive approach to preventing ex-employee user accounts from creating any more security risks, it is recommended that you create a "Leavers" deny access policy. This will ensure that if a malicious actor comprises a stale account to gain access to anything in your environment, they will be automatically denied access.



Screenshot #3: Deny access policy to prevent stale user access

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 **Static Based** for the policy type and beside **User and Group**, type either "Leavers" or the name your organization uses for employees who are leaving or have left. Next, under **Action**, choose **Deny**.

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

For more information, visit the Silverfort Documentation Centre or get in touch with your assigned Customer Success Manager.