Tag Types

Scirge collects accounts and application metadata that are discovered by the Endpoint Browser Extension based on policies. Tags are associated based on password hygiene, usage trends, cloud intelligence, and correlation of events. Tags can be configured, and unique Tags can be created based on Custom critera as well.

ACCOUNT TAGS

Tags relating to accounts are mainly concerned with password hygiene and usage trends. Some Tags can be customized, for example, to define password complexity, expiration, or blacklists.

Weak Password
Blacklisted Password
LDAP Password Reuse
Password Reuse
Common Password
Shared Account
Breached Password
Underutilized
Top Usage
Very Weak Password
Password Expired
Password Autofill
New
Password Complexity
Abandoned
Very Strong Password
Strong Password
Moderate Password

APPLICATION TAGS

Application Tags are showing usage trends and website reputation such as domain age, missing legal terms, or when they are blacklisted on spam lists.

Blacklisted Domain
SSL Issues
Abandoned
Untrusted
Missing Legal
New
Popular
Managed
Underutilized
Non-password Accounts Only
In-house
Fresh Domain
Trending

PEOPLE TAGS

People Tags show AD/LDAP-related password hygiene and account usage-related information, as well as potential signs of fraud.

Breached LDAP Password
Strong LDAP Password
Weak LDAP Password
Identity Misuse Victim
Disabled LDAP Account
LDAP Password Reuse
Moderate LDAP Password
Power User
Blacklisted LDAP Password
Password Hygiene
Deleted LDAP Account
Identity Misuse
Common LDAP Password
Very Strong LDAP Password
Inactive LDAP Account Reuse
Very Weak LDAP Password
New
LDAP Password Complexity
VIP

CUSTOM TAGS

Custom Tags can be based on the correlation of other tags, manual assignment, and LDAP group membership.

AD_Administrators
Training advised
Finance
Suspected Phishing for VIP

SCIRGE

Tags by Use Cases

Different Tags can be used to identify indicators of different risk types. Protection against account takeovers and hacking is based on password hygiene checks, while visibility and compliance are supported via complexity rules and account and application usage Tags.

ACCOUNT AND PASSWORD PROTECTION

These tags reveal when unsecure passwords are created, or when accounts are misused from a security or compliance perspective.

Suspected Phishing for VIP
LDAP Password Reuse
Password Reuse
Fresh Domain
Common Password
Breached Password
Very Strong Password
AD_Administrators
Very Weak LDAP Password
Password Complexity

SHADOW IT DISCOVERY

Trends of application usage and indicators of risky websites are tagged for visibility into Shadow IT.

Developers
Abandoned
SSL Issues
Untrusted
Popular
Missing Legal
Blacklisted Domain
Managed
In-house
Underutilized
Fresh Domain
Trending
Finance
Power User
New

GOVERNANCE, RISK, AND COMPLIANCE

Logins on risky websites, usage of weak or shared passwords, and impersonating other employees are all indicators of misconduct and violation of regulations.

Breached LDAP Password
Identity Misuse Victim
Blacklisted LDAP Password
Shared Account
Disabled LDAP Account
Deleted LDAP Account
Identity Misuse
Password Hygiene
Password Autofill
Common LDAP Password
Abandoned
VIP
Training advised
LDAP Password Complexity
AD_Administrators

Correlations

Some Tags speak for themselves, but correlating them creates indicators that are more than the sum of its parts. These combinations can be set up using various alerting methods to warn employees or security operators, or utilized to assign additional Tags. Here are just some examples.

POTENTIAL PHISHING

Password reuse or new accounts on a recently registered, risky, or first seen domain indicates that a user may have fallen victim to a phishing attack.

SSL Issues | Fresh Domain | New | Untrusted | Blacklisted Domain + LDAP Password Reuse | Password Reuse | New

HIGH RISK PASSWORD USAGE

Reusing passwords is risky enough, but when the password already has signs of weakness, it makes it crucial.

LDAP Password Reuse | Password Reuse + Breached Password | Very Weak Password | Password Complexity | Blacklisted Password

UNWANTED APPLICATIONS

Employees are concerned about getting their job done. But when Shadow IT applications emerge or are left behind, management must understand if there are any compliance risks or overheads created.

Popular | Underutilized | Trending | Abandoned + SSL Issues | Missing Legal | Untrusted

PROTECTING PRIVILEGED USERS

When accounts of high privilege user or ex-employees are utilized by other, it's an indicator of potential impersonation or internal fraud.

Disabled LDAP Account | Identity Misuse Victim + VIP | Developers | AD_Administrators

IDENTIFYING RISKY BEHAVIOUR

Employees with a high number of accounts with low overall password qualities, using unsanctioned password managers or shared accounts should be identified for further education.

Power User | VIP | Password Hygiene + Training advised | Suspected Phishing for VIP | Shared Account | Password Autofill

SCIRGE