



Single Sign-On (SSO)

UNIFIED ACCESS MANAGEMENT FOR SUREVIEW OPERATORS PLATFORM

Single Sign-On (SSO) lets your team sign in to SureView accounts using their existing corporate credentials—no separate usernames or passwords required. SureView supports both OpenID Connect and SAML 2.0, integrating with the identity platform your organization already runs.

WHY IT MATTERS

Security operations teams touch many systems every shift. Separate SureView credentials create friction at sign-in, generate password reset requests, and leave IT managing accounts that should already be centralized. SSO puts access control back where it belongs—inside the identity provider you already manage.

BENEFITS

- **One login, every system:** Your team signs in to SureView with the same credentials they use everywhere else—no additional passwords to manage or reset.
- **Offboarding in one step:** Disabling a corporate account revokes SureView access immediately—no separate cleanup required.
- **Fewer help desk tickets:** Password resets, account lockouts, and SureView access requests disappear from the IT queue.
- **New starters productive from day one:** SSO provisions first-time users automatically—no wait for IT to set up a SureView account.
- **No vendor lock-in:** SAML 2.0 support means SureView works with the identity provider your organization already has in place.
- **Always accessible:** Administrators retain a direct login path—operations don't stall if the identity provider has an outage.



KEY FEATURES

- **Multi-Protocol Identity Support:** SureView supports both SAML 2.0 and OpenID Connect, so organizations can connect any compatible identity provider—including Okta and Microsoft Azure Active Directory—without custom development.
- **Direct Login Experience:** When operators land on SureView, they go straight to your identity provider—and land in the event queue the moment they authenticate. No SureView login screen, no extra steps.
- **Automatic User Provisioning:** New team members log in via SSO and get a SureView account on first login—permissions pulled from your Active Directory domain.
- **Single Sign-Out:** Logging out of SureView simultaneously signs the user out of the identity provider—reducing the risk of open sessions on shared workstations. Supported on OpenID Connect integrations.
- **Administrator Bypass Access:** Administrators retain a direct login path to SureView independent of the SSO provider—so the system stays accessible even if the identity provider is unavailable.
- **Centralized IT Configuration:** All SSO settings are managed through the SureView System Settings page, accessible to system administrators only. No file editing required for most deployments.

