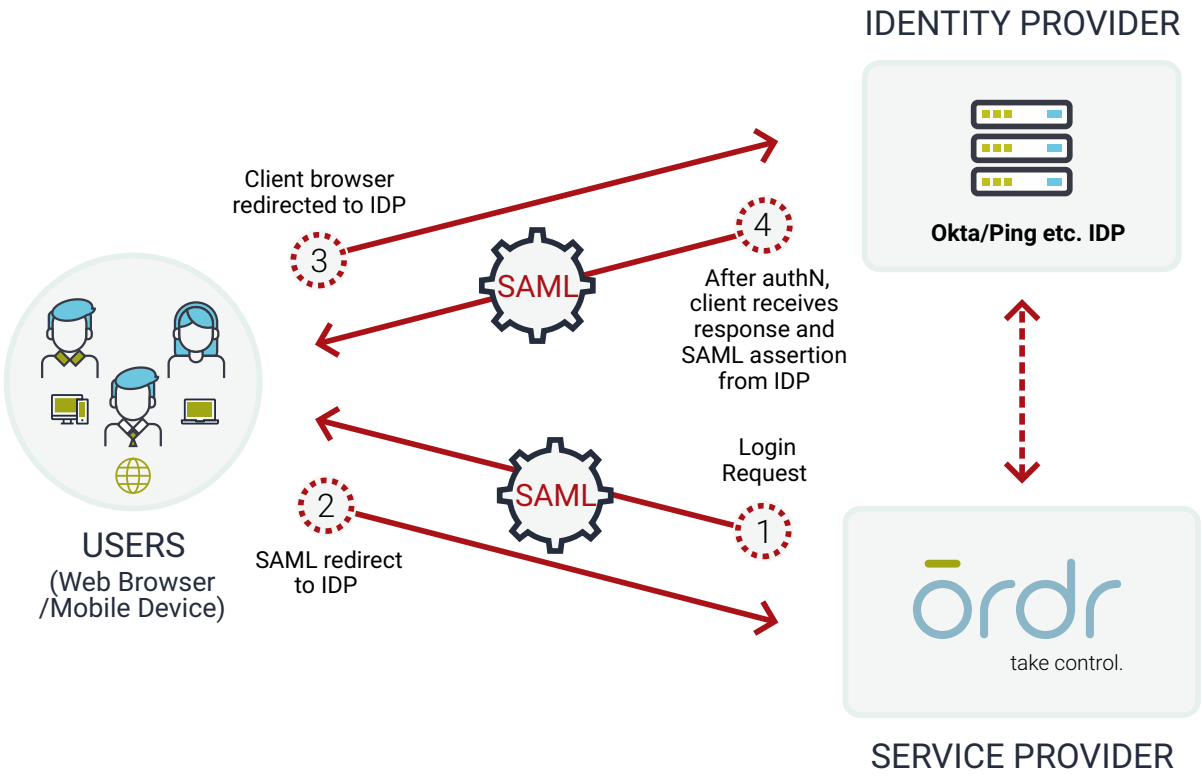
Efficient SSO via SAML Integration

Quick Access to Ordr Systems Control Engine (SCE)

IT and Security teams face increasingly complex demands as their large workforces transition between full-time, part-time, outsourced, on-premise, and work-from-home models. Throughout these transitions, consistent and secure access to business applications remains a constant requirement, and single-sign on (SSO) is critical to credential hygiene and management. With the proper implementation of SSO, users can access these applications at any time, unconstrained from location and from any approved device.

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IDPs) to pass authorization credentials to service providers (SP). SAML enables SSO, a term that means users can log in once, and those same credentials can be reused to log into other service providers.



Ordr Systems Control Engine (SCE)

With the Ordr SSO integration into existing IDPs like Okta, Ping Identity, Oracle, etc., organizations will have centralized management and access to Ordr SCE. Ordr SCE is an IoT and unmanaged device security platform that will discover every connected device, profile device behavior and risks, and automate response. Ordr not only identifies devices with vulnerabilities, weak ciphers, weak certificates, and active threats, but also those that exhibit malicious or suspicious behaviors. Finally, Ordr automates response for security and networking teams, such as dynamically generating policies and enforcing them on existing infrastructure, or alerting and triggering a specific security or operational workflow.

SAML Integration with Ordr SCE

The Ordr SCE SAML integration supports Service Provider-initiated SSO. This involves the SP creating a SAML request, forwarding the user and the request to the IDP, and then, once the user has authenticated, receiving a SAML response & assertion from the IDP.

When the SP receives a SAML response it will fetch the stored request ID and relay state values and check them against the SAML responses InResponseTo value and relay state, respectively.

This ensures Ordr receives an expected assertion that is proven by the presence of the request ID and relay state and that the response is intended for Ordr by matching the request ID and relay state.

When using SP-initiated SSO, a modern SAML solution will do the following:

- Generate a request ID and include it in the SAML request message
- Generate a relay state either random application state or just as a simple Cross-site Request Forgery mechanism and include it in the SAML request URL
- Securely store the two values before redirecting to the IDP

Benefits

Quick and secure access to enterprise applications, websites, and data for which they have permission for increased productivity

Proper provisioning of access for users

Reduction in the amount of credentials one user has for multiple vendors

Case Study

A large healthcare organization with more than 18 hospitals, 220 outpatient locations, 6,000 beds, and 20 patient-centered institutes, serving more than 2.4 million patients, and employing more than 67,500 individuals, is addressing their managed and unmanaged device security risks.

For their environment, they were looking not only to address visibility of managed and unmanaged devices, the ability to automate policy creation, understand behaviors and risk, but they were looking to address multiple stakeholders for the Ordr instance. Using the recent enhancement to support SAML 2.0 as a service provider within Ordr SCE, allows this customer to authorize diverse departments efficient and secure access. They have Security, IT and BioMed involved in using the rich device context to inform business and operational decisions.

Ordr's real-time dashboard and essential device insights, such as passive and continuous device inventory, mapping of device communication, device risk analysis, and device utilization made Ordr easy to deploy and access for all members of their team.

About Ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. For more information, visit www.ordr.net and follow Ordr on Twitter and LinkedIn.